UNIVERSIDAD GERARDO BARRIOS

FACULTAD DE POSTGRADO Y EDUCACIÓN CONTINUA

MAESTRÍA EN DERECHO PENAL

TRABAJO PARA OPTAR AL GRADO DE MAESTRO EN:

DERECHO PENAL

"LÍMITES A LA IMPLEMENTACIÓN DE LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS, EN EL DELITO DE REVELACIÓN INDEBIDA DE DATOS O INFORMACIÓN DE CARÁCTER PERSONAL"

PRESENTADO POR:

LIC. HÉCTOR DAVID ARGUETA GRANADOS

ASESOR

MSC. LIC. JUAN CARLOS PAZ HERNÁNDEZ

EL SALVADOR, SAN MIGUEL, 3 DE JUNIO DE 2021

RECTOR

MSC. LIC. JOSÉ SALVADOR ALVARENGA RIVERA

FISCAL

MSC. LIC. NAPOLEÓN ALBERTO RÍOS-LAZO ROMERO

DECANO

MSC. LIC. MIGUEL ANTONIO FLORES CASTRO

AGRADECIMIENTOS

A DIOS, por todas las bendiciones que ha brindado a mi vida, por la fortaleza e inteligencia necesarias que me ha dado a lo largo de mi formación académica, y por haberme permitido alcanzar con éxito una de las metas y sueños, como lo es la obtención del título de master. Todo se lo debo a Él.

A MIS PADRES, María Amalia Argueta Ramos y Modesto Majano Granados, de grata recordación, por siempre animarme, por ser ese apoyo incondicional y luchar de la mano conmigo para ser un profesional con éxito y lograr un peldaño más en mi carrera como profesional; gracias por su amor, apoyo y sacrificio en todo este tiempo, por ser mis ejemplos para salir adelante y por los consejos que han sido de gran ayuda para mi vida; por tanto, este triunfo, es el resultado de lo que me han enseñado en la vida, y va dedicado a ustedes.

A MI HERMANA, Rosa Elizabeth Argueta Granados, por apoyarme en mi formación profesional que me permitió optar a una especialización de mi carrera, por estar siempre a mi lado siempre en los momentos que más he necesitado; siempre, siempre, ha estado incondicionalmente conmigo.

A MI QUERIDO SOBRINO, Wilber Neftalí Umanzor Argueta, que ha hecho las veces de un hermano, que a pesar de ser un jovencito, ha estado conmigo en los momentos de alegría y tristeza.

A MI HERMANO, Oscar Alberto Villalta Argueta, por ser un buen hermano, darme buenos consejos, aliento y ánimo, así como su apoyo al decirme que soy diferente y que luche constantemente, día a día, que nunca me rinda, que yo puedo seguir siempre adelante.

A TODOS MIS FAMILIARES, que siempre creyeron en mi y han sido siempre mi apoyo incondicional en los momentos buenos y malos; también este nuevo triunfo va dedicado a ustedes.

A MI AMOR, Ivonne Eunice de la Paz Chévez de Argueta, por ser mi apoyo incondicional, por estar siempre a mi lado, en los momentos más difíciles y en los momentos

más felices de mi vida. Mil gracias por ser la mujer que es y espero tener su apoyo y su amor durante toda mi vida y este triunfo es suyo y mío.

A MI ASESOR, por recibirme y darme su apoyo eficiente en el momento que más lo necesitaba. Comprometerse conmigo, en un momento no convencional, habla muy bien de su excelente calidad humana y profesionalismo, atributos puestos de manifiesto en esa labor tan abnegada y noble, como es la docencia universitaria, la cual desempeña con una alta eficiencia. Muchas gracias por la huella imperecedera que ha dejado en mí. Bendiciones de lo Alto.

CONTENIDO

INTRODUCCIÓN

Recientemente El Salvador entró en la ruta de legislar los hechos delictivos cometidos a través del uso de Tecnologías de la Información y la Comunicación (TICs) mediante la aprobación de la Ley Especial Contra los Delitos Informáticos y Conexos[1], con la finalidad de caracterizar la diversidad de hechos punibles y tipificarlos como delitos. No obstante, se han generado nuevos desafíos para la investigación y la tipificación de esos hechos cometidos mediante el uso de la ciberdelincuencia.

En la presente investigación se abordó el hecho que dentro de los delitos informáticos, que contiene la Ley Especial Contra los Delitos Informáticos y Conexos, se trató el punto que el Delito de Revelación Indebida de Datos o Información de Carácter Personal, es el más cometido por la población, lo cual se pudo constatar a través de datos estadísticos por parte de la Unidad de Acceso a la Información Pública (UAIP) de la Policía Nacional Civil y Fiscalía General de la República[2], lo que contrasta con el hecho que no existe un tratamiento claro, ni tampoco un protocolo que contenga los lineamientos idóneos que permita identificar los procedimientos diferenciados, trato o enfoque individualizado de ese Delito, respecto a la generalidad del cometimiento de otros delitos que no contempla la LEDIC.

Puntualmente se procedió a investigar en la Policía Nacional Civil y la Fiscalía General de la República, con el objetivo de identificar los recursos humanos y medios materiales como dispositivos electrónicos especializados, diversidad de programas de rastreo, tipo de capacitaciones, procedimientos de investigación, herramientas técnicas, jurídicas y científicas con las que realizan la investigación de los delitos informáticos en general, especialmente en el Delito de Revelación Indebida de Datos o Información de

[1] Aprobado por la Asamblea Legislativa por medio del Decreto Legislativo N°260, del día 26 de febrero de 2016, publicado en el D. O. No. 40, Tomo No. 410.

[2] Unidad de Acceso a la Información pública/ OIR-PNC (anexo 3 y 4) y Fiscalía General de la República, Unidad de Acceso a la Información Pública (Anexos 5, 6 y 7)

Carácter Personal, así como también el conocimiento y el procedimiento de la referida Ley.

Para conocer las competencias del personal de la PNC y la FGR, en cuanto al conocimiento, comprensión en la investigación y en el procedimiento de judicialización de los delitos tipificados en la LEDIC, se indagó sobre el grado académico de los investigadores, cómo se conformaban los equipos de trabajo, tipo de formación recibida, uso de herramientas técnicas y científicas, así como el tipo de limitaciones que se tiene en la investigación del Delito de Revelación Indebida de Datos o Información de Carácter Personal, además por qué es el más cometido por la población del municipio y departamento de San Miguel, y si existe o no impunidad.

Por no encontrar información sobre las herramientas técnicas científicas que utiliza la Policía Nacional Civil de San Miguel, para la investigación de los delitos informáticos tipificados en La Ley Especial Contra Delitos Informáticos y Conexos, se buscó información en la sede central en San Salvador, encontrando que existe una unidad especializada, que cuenta con un equipo completo de investigación de estos delitos; sin embargo, no se tuvo acceso a conocer las herramientas utilizadas para persecución e investigación de estos delitos, debido a que es información de carácter reservado, fundamentado en memorándum[3] SIN/DCI/0232/2020 de fecha 16 de abril de 2020, suscrito por el Subdirector de investigaciones, Comisionado Juan Carlos Martínez Marín.

En razón de lo anterior, en el capítulo I se aborda la situación problemática, identificándose las limitaciones que existen en la Fiscalía General de la República y la Policía Nacional Civil, para detectar e investigar los hechos cometidos mediante el uso de las herramientas tecnológicas y de la comunicación, lo cual es más evidente en dichas instituciones del municipio de San Miguel; tal situación se comprobó mediante los registros estadísticos desde el año 2018 y que aún se mantienen al 2020, donde se reporta que el delito más cometido es el de “Revelación Indebida de Datos o Información de Carácter Personal”

[3] SIN/DCI/0232/2020 de fecha 16 de abril de 2020 PNC/OIR; anexo 2.

En el capítulo II se habla de los antecedentes históricos de cómo surgió la necesidad de legislar el tema de las nuevas tecnologías de la comunicación, que han dado lugar al cometimiento de hechos delictivos; se describen las diferentes relaciones con organismos internacionales, con el fin de apoyar esas iniciativas; se describe el desarrollo de la temática y los obstáculos en el país, así como también se encuentran definiciones de términos propios de la jerga informática, al igual que de los delitos más relevantes de la LEDIC, tipificación del Delito en estudio en El Salvador y en el contexto Latinoamericano.

CAPÍTULO I

PROBLEMA DE INVESTIGACIÓN

1.1.1 SITUACIÓN PROBLEMÁTICA

El Programa Global de Ciberdelito de UNODC ha colaborado, desde el año 2014, en el fortalecimiento institucional del Sector Justicia de El Salvador, bajo el proyecto "Fortalecimiento de las capacidades de la Policía Nacional Civil de El Salvador en la identificación efectiva e investigación de casos de cibercrimen". Este Programa buscó iniciar, dinamizar y fortalecer la investigación y persecución penal de los delitos informáticos/cibercrimen.[4] Entonces, si se pretende evitar la impunidad en esta clase de hechos, resulta indispensable la aplicación de actividades técnicas y periciales informáticas; pues, por tratarse de delitos no convencionales, estos no podrían ser abordados con las herramientas tradicionales del Derecho Penal.

Asimismo, pese a los esfuerzos de la Oficina de las Naciones Unidas contra la Droga y el Delito[5], que es la encargada de brindar asistencia técnica a los Estados

---

4 UNODC ROPAN (Oficina de las Naciones Unidas contra la Droga y el Delito para Centroamérica y el Caribe) Fiscalía General de la República de El Salvador, Escuela de Capacitación Fiscal. 2018. 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, pág.10

5 En septiembre de 2009 y con el objetivo de ofrecer un mayor servicio a los Estados Miembros de la región, la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) decidió brindar apoyo a las operaciones de su Oficina Regional en México (Oficina que cubría Centroamérica y el Caribe en ese entonces), a través del establecimiento de una Oficina Regional de Programas en Panamá (RPOPAN). Dicha Oficina fue inaugurada en junio de 2010. Los nuevos desafíos y amenazas enfrentados por Panamá y el resto de los países de la región en los años siguientes, obligaron a RPOPAN a evolucionar hasta convertirse en Oficina Regional para Centroamérica y el Caribe en Panamá (UNODC ROPAN).
UNODC ROPAN, que cubre 24 países de Centroamérica y el Caribe y trabaja con tres de los seis idiomas oficiales del Sistema de las Naciones Unidas (español, Inglés y Francés), inició sus operaciones como Oficina Regional en marzo de 2012.
El mandato de UNODC consiste, principalmente, en proporcionar asistencia técnica a los Estados Miembros para fortalecer sus capacidades en la lucha contra la delincuencia organizada y el tráfico de drogas. En este contexto, UNODC ROPAN presta especial atención a las necesidades específicas de los países de Centroamérica y el Caribe, con el fin de prestar una asistencia técnica hecha a medida, coherente y eficaz que permita hacer frente a los retos planteados por estos fenómenos en la región.
Las operaciones de UNODC alrededor del mundo son financiadas gracias a los aportes de la comunidad de donantes y están guiadas por una serie de tratados, convenciones y normas internacionales.
ROPAN ha incorporado los principios básicos de UNODC para elaborar estrategias y programas a nivel nacional, regional e inter- regional. Estas estrategias y programas están diseñados para apoyar a los Gobiernos en los distintos sectores vinculadas con el mandato de UNODC, apuntando al mismo tiempo a lograr los Objetivos de Desarrollo del Milenio. UNODC ROPAN posee una amplia cartera de proyectos enfocados en áreas tales como Reforma Penitenciaria, Seguridad Aeroportuaria y Control de Contenedores, Trata de Personas y Tráfico Ilícito de Migrantes, Reducción de la Demanda de Drogas, Delincuencia Organizada, Investigación y Análisis de Tendencias, Seguridad Ciudadana y Corrupción.
Los programas de UNODC ROPAN que se enfocan en las áreas previamente mencionadas, son llevados a cabo con un enfoque particular, basado en tres pilares de trabajo principales:
1. Proyectos de asistencia técnica en campo diseñados para mejorar las capacidades de los Estados Miembros en la lucha contra el tráfico de drogas y la delincuencia transnacional organizada.

Miembros en la lucha contra el tráfico de drogas, la delincuencia organizada, la corrupción y los desafíos planteados por estos fenómenos, todavía son evidentes en la Policía Nacional Civil y Fiscalía General de la República, las limitaciones para detectar e investigar los hechos cometidos bajo el uso de herramientas de las tecnologías de la información y comunicación, tales limitaciones son aún más determinantes en el municipio de San Miguel.

Los funcionarios de la Policía Nacional Civil y Fiscalía General de la República en el municipio y departamento de San Miguel, carecen de una unidad especializada para la investigación de los delitos informáticos; en consecuencia, no hay acceso a las herramientas tecnológicas para la identificación, investigación y juzgamiento de los hechos constitutivos, tanto es así que la función de la Policía Nacional Civil, se limita únicamente a ser receptora de denuncias y trasladarlas hacia la Fiscalía General de la República y ésta la deriva hacia la sede central en San Salvador, generando retrasos en los procesos.

Desde la aprobación de la Ley Especial Contra Delitos Informáticos y Conexos (LEDIC) el día 26 de febrero de 2016, mediante el D. L. No. 260, publicado en el D. O. No. 40, Tomo No. 410, se resolvió el vacío normativo que existía en esta materia, pues se lograron configurar los hechos punibles relacionados con la ciberdelincuencia. Sin embargo, se generaron nuevos desafíos para la persecución de este tipo de delitos, por cuanto, la referida normativa exige contar con la capacidad técnica y jurídica en la

---

2. Trabajo de investigación y análisis que permita incrementar el conocimiento y la comprensión de las problemáticas planteadas por el tráfico de drogas y la delincuencia transnacional organizada y que sirvan como base para la toma de decisiones políticas y operativas.
3. La labor normativa diseñada para ayudar a los Estados Miembros en la ratificación y aplicación de tratados internacionales; el desarrollo de legislación nacional en materia de drogas, la delincuencia y el terrorismo; y la prestación de servicios sustantivos y secretariales a organismos relevantes.
A nivel nacional, UNODC ROPAN apoya a los Gobiernos de los Estados Miembros en el desarrollo y la implementación de iniciativas prioritarias. Los programas integrados de seguridad y justicia tienen como objetivo el fortalecimiento de los estructuras del Estado en la lucha contra el tráfico ilícito de drogas, la corrupción, el lavado de dinero y el crimen organizado, así como también el refuerzo de la seguridad nacional. UNODC ROPAN colabora estrechamente con varias instituciones gubernamentales, las cuales tienen un rol fundamental en la elaboración e implementación eficiente de los diversos programas ejecutados bajo la dirección de la Oficina.
Desde una perspectiva regional, la UNODC ROPAN desarrolla sus operaciones en estrecha cooperación, tanto con los Estados Miembros de la región, como con organizaciones regionales tales como la Comunidad del Caribe (CARICOM, por sus siglas en inglés) y el Sistema de la Integración Centroamericana (SICA). De igual manera, la Oficina continúa brindando apoyo y asistencia técnica en la elaboración de políticas regionales de seguridad y de justicia en cada región, así como diversas iniciativas para contrarrestar la delincuencia transnacional organizada.
A nivel inter-regional, UNODC ROPAN actúa para promover y facilitar la cooperación, no sólo entre Centroamérica y el Caribe, sino también entre estas y otras regiones alrededor del mundo, a través de la implementación de programas globales (UNODC Centroamérica y el Caribe, 2020)

utilización de tecnologías de la información y comunicación, tanto en la comisión de delitos, como en su investigación.

Las estadísticas[6] muestran que, desde la implementación de la LEDIC, en febrero de 2016 hasta febrero de 2018 (cabe mencionar que solo se ha visto en pleno funcionamiento durante el año 2017) se contabilizaron 568 delitos, de los cuales 165 corresponden al delito de revelación indebida de datos o información de carácter personal.

> De ese total de 568, en la Fiscalía General de la República solo en un aproximado del 10% de los casos se ejercerá la acción penal presentándose requerimiento, de estos hechos en los que se ejerce la acción penal, apenas la mitad de los mismos llegarán a la fase de presentación de Dictamen de Acusación, y las posibilidades de condena son aún más escasas. Es importante conocer porqué tan pocos de los delitos que ingresan y conoce el ente fiscal, son requeridos ante los tribunales (10% de los ingresados), debemos recordar en este punto que la investigación de la delincuencia informática tiene dificultades añadidas en comparación al resto de delitos -transnacionalidad, horizontalidad y opacidad de las redes sociales, entre otros - (Feusier, 2018, p.67).

Concretamente se tiene la información que durante el período del 2016 al 2017, se tuvo un consolidado para tales años como sigue: en el año 2016, casos ingresados, 149; casos en los que se requirió, 8; casos en los que se presentó dictamen, 2; condenas logradas, 0 y absoluciones, 0. Ahora bien, los datos en el 2017 fueron: Casos ingresados, 380; casos en los que se requirió, 42; casos en los que se presentó dictamen, 20; condenas logradas, 2 y absoluciones, 2.

De acuerdo a los datos existentes en investigaciones, por ejemplo, la promovida por el Consejo Nacional de la Judicatura, en el trabajo realizado en el año 2018 por Feusier y Martínez, con relación a los delitos informáticos, se evidencia que, del total de éstos, el que presenta el mayor número de denuncias, en la Fiscalía, es el delito de Revelación Indebida de Datos o Información de Carácter Personal, situación que se

---

[6] Aplicación y Contenido de la Ley Especial contra la Delincuencia Informática y Conexos. Concurso de Investigación CNJ, "Fomentando a investigación para mejorar la Administración de Justicia. Oswaldo Feusier y Emely Martínez, pág.81-82

mantiene en la actualidad, tanto en la Policía Nacional Civil como en la Fiscalía General de la República, y aún de mayor importancia es el verificar la reducida cantidad de casos judicializados, de lo cual surge la inquietud de investigar por qué existe esa pasividad legal de parte de esas entidades, situación que establece las bases para preguntarse por qué no se judicializan esas denuncias, cuáles serán los errores cometidos en las investigaciones, por qué hay falta de acceso a la protección jurisdiccional de las víctimas, falta de formación especializada en los agentes de la Policía Nacional Civil y la Fiscalía General de la República para investigar el delito, falta de herramientas y recursos técnicos para realizar las investigaciones

También, debe valorarse que se trata de comportamientos que apenas comienzan a medirse, por tratarse de una ley cuya vigencia inicia en el 2016. Sin embargo, de continuarse con esta tendencia habría que concluirse que la LECDIC a pesar de sus muchas tipificaciones, logra escasos resultados, por los menos, si por resultados entendemos condenas. Estos resultados generan en la población desconfianza para denunciar este tipo de delitos, situación que se suma a los limites u obstáculos en la aplicación efectiva de la Ley Especial Contra los Delitos Informáticos y Conexos, y en consecuencia la efectividad es mínima pues la mayoría de estos delitos quedan impunes.

1.1.2 DELIMITACIÓN

La delimitación del trabajo, en cuanto al tipo de investigación, se propone de campo y de naturaleza jurídica, ya que se pretende identificar el tipo de herramientas tecnológicas y capacidad técnica y jurídica que tienen los funcionarios del Departamento de Investigaciones de la PNC, Unidad Especializada de la Fiscalía General de la República; lo cual determina su nivel de eficacia en cuanto de minimizar los niveles de impunidad del delito Revelación indebida de datos o información de carácter personal.

1.1.3 ENUNCIADO DEL PROBLEMA

En la ciudad de San Miguel, de acuerdo a datos estadísticos[7] del período que va de enero de 2018 hasta febrero de 2020, existen 147 denuncias de delitos informáticos; de

[7] Datos estadísticos proporcionados por la Fiscalía General de la República, Unidad de Acceso a la Información Pública. Solicitud N°151-UAIP-FGR-2020.

éstos el que más incidencia tiene, con 55 denuncias, es el Delito de Revelación Indebida de Datos o Información de Carácter Personal. De ese total de 147 denuncias, 81 casos se encuentran activos, es decir en investigación, de los cuales, 36 corresponden al delito en mención, posicionándose como el más denunciado. La estadística reporta que, en el periodo antes señalado, únicamente se han presentado 2 dictámenes, que además no corresponden al delito más denunciado, objeto de esta investigación.

Esta situación permite preguntarse que si bien es cierto existen investigaciones de la Policía y Fiscalía ¿por qué es tan poca la cantidad de casos que se investigan y se judicializan?; ¿por qué si existe una mayor incidencia en las denuncias del Delito de Revelación Indebida de Datos o Información de Carácter Personal, no se tiene claridad del debido proceso que se le da, ya que no hay evidencia de casos judicializados, ni de condenas, ni de absoluciones para este delito?

1.1.4 JUSTIFICACIÓN

El Cibercrimen actualmente se posiciona como una actividad criminal muy lucrativa como el narcotráfico y la comercialización de armas, pero con la ventaja que es invisible al resto de ciudadanos. Debido a su transnacionalidad, facilita el uso de internet como mecanismo para la ejecución de sus actividades criminales.

El cibercrimen, aumentará cada año por el avance de la tecnología y del mercado; por lo tanto, se hace necesario investigar las necesidades y actualización constante de los investigadores de la Fiscalía y Policía Nacional Civil, a efecto de dotar de seguridad a los ciudadanos que, cada vez más, utilizan el internet para realizar sus actividades cotidianas, situación que aprovechan ciertas personas para delinquir principalmente en la revelación de datos o información de carácter personal.

Las autoridades competentes de este tipo de investigaciones en la ciudad de San Miguel, no tienen claro del porqué no se realizan las investigaciones del Delito de Revelación Indebida de Datos o Información de Carácter personal, razón por la cual resulta importante hacer un estudio que permita identificar las limitantes en la investigación, tipo de Herramientas y el grado de formación especializada técnica/científica, en la Policía Nacional Civil y en la Fiscalía General de la República, de San Miguel.

1.1.5 OBJETIVOS

1.5.1. General

Identificar los límites que tienen la Policía Nacional Civil y la Fiscalía General de la República en la ciudad de San Miguel para la investigación del delito de Revelación Indebida de Datos o Información de Carácter Personal, art. 26 de la Ley Especial contra los Delitos Informáticos y Conexos.

1.5.2. Específicos

1.5.1.1. Identificar el tratamiento que se le da al delito de Revelación Indebida de Datos o Información de Carácter Personal (siendo éste el más denunciado) en la Fiscalía General de la República y en Policía Nacional Civil, de la ciudad de San Miguel.

1.5.1.2. Mostrar el tipo de herramientas y técnicas jurídicas que existen para la investigación del Delito de Revelación Indebida de Datos o Información de Carácter Personal, en la Fiscalía General de la República y Policía Nacional Civil de San Miguel y cuáles son las limitantes que tienen estas herramientas.

1.5.1.3. Plantear los límites que tienen la Policía Nacional Civil y la Fiscalía General de la República en la ciudad de San Miguel para la investigación del delito de Revelación Indebida de Datos o Información de Carácter Personal, art. 26 de la Ley Especial contra los delitos informáticos y conexos.

CAPITULO II

MARCO TEÓRICO

2.1. ANTECEDENTES HISTÓRICOS

2.1.1 Delitos informáticos en América Latina

> Según el Departamento de Prensa de la Organización de los Estados Americanos (OEA), el auge de las tecnologías del último siglo ha traído consigo innumerables avances para la humanidad, pero también otra serie de retos para las autoridades, legisladores e investigadores en las Américas, quienes han tenido que centrarse cada vez más en la persecución y sanción de los delitos cibernéticos, como la pornografía infantil, robo de identidad, acoso (OEA, 2016a).

"La evolución tecnológica…, ha incidido en la ejecución de actividades delictivas, donde la tecnología es utilizada como medio para cometer delitos comunes y de crimen organizado, o bien, cuando la misma se convierte en el objeto de agresión" (Iberoamericana, Grupo E-Justicia Cumbre Judicial, 2018, p. 1).

> Las tendencias futuras en el incremento del cibercrimen estas orientadas a actividades como: el Crime-as-a-Service*,* Ransomware*,* Uso criminal de datos, *Fraude de pago,* Abuso sexual infantil en línea, Abuso de la Darkenet, Ingeniería Social, Monedas virtuales, así como el ataque a infraestructuras críticas, lo cual pone en peligro vidas humanas y la economía de los países. (Iberoamericana, Grupo E-Justicia Cumbre Judicial, 2018, p. 2).

Según estimaciones del Registro de Direcciones de Internet de América Latina y Caribe (LACNIC), el cibercrimen le cuesta a la región alrededor de 90.000 millones de dólares año (OEA, 2016b).

Congruente con lo anterior, la empresa Northon Ciberseguridad (2016) “A nivel mundial las perdidas superaron los 125.900 millones de dólares (p.3).

> LACNIC, es una organización no gubernamental internacional, instituida en Uruguay en el año 2002, se encarga de establecer el Registro de Direcciones de Internet de América Latina y Caribe, cuya función es asignar y administrar los recursos de numeración de Internet (IPv4, IPV6) números autónomos y resolución inversa para región. (LACNIC, s.f.)
>
> Por eso, en 1999 los Ministros de Justicia y Procuradores Generales de las Américas decidieron reunir en el marco de la Organización de los Estados Americanos (OEA) un grupo de expertos sobre delito cibernético para: realizar un diagnóstico de la actividad delictiva vinculada a las computadoras y la información en los Estados miembros.
>
> Hacer un análisis de la legislación, las políticas y las prácticas nacionales sobre cibercrimen.
>
> Identificar las entidades nacionales e internacionales que tienen experiencia en la materia; y
>
> Buscar mecanismos de cooperación para combatir flagelo.
> (OEA, 2016c)

Esta entidad se conoce como el Grupo de Trabajo en Delito Cibernético de las Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas (REMJA)[8] (OEA, Departamento de Cooperación Jurídica, 2020 OEA) que se reúne bianualmente para mejorar y fortalecer la cooperación jurídica y judicial (OEA,

[8] REMJA: Son las reuniones de Ministros de Justicia o de Ministros o Procuradores Generales de la Américas, celebradas periódicamente bajo los auspicios de la Organización de los Estados Americanos (OEA) desde el año 1997, con el propósito de fortalecer la cooperación jurídica y judicial entre los Estados del Hemisferio Americano. Dicha cooperación, es un mecanismo mediante el cual la comunidad internacional puede, de una manera más efectiva, enfrentar el crimen internacional. Los Estados miembros de la OEA han reconocido siempre la importancia de la cooperación judicial y de otras formas de cooperación en materia penal, bajo la óptica de que la investigación y la represión de delitos para la protección del ciudadano y el mantenimiento de la paz y el orden público constituyen objetivos esenciales en toda sociedad organizada y que la lucha para alcanzar esos objetivos no se puede restringir actualmente a límites nacionales, por cuanto es evidente que la delincuencia transnacional organizada no cuenta con esas barreras para cometer sus crímenes, los cuales ya no solo afectan a los países individualmente considerados sino a la comunidad internacional en general. Para el logro de sus propósitos, se han creado en el marco de las REMJA grupos de trabajo que se ocupan de tareas concretas, tales como los de Expertos en Asistencia Judicial Mutua en Materia Penal y Extradición; Grupo de Expertos Gubernamentales en Materia de Delito Cibernético; y Autoridades Responsables de las Políticas Penitenciarias y Carcelarias.

Departamento de Cooperación Jurídica, 2020 OEA)[9] entre los Estados del Hemisferio.

El diagnóstico que salió de este proceso demostró que quizás la mayor dificultad que enfrentan los países de la región en cuanto al delito cibernético es la carencia de entidades especializadas en la materia que tengan la facultad para investigar y perseguir la comisión de este delito y la falta de capacitación suficiente para adelantar una labor exhaustiva y (OEA, 2016d).

En respuesta a este reto, la OEA (OEA, 2016e) con el apoyo de algunos países de la región, decidió empezar a desarrollar talleres y entrenamientos para capacitar a los jueces y magistrados de los poderes judiciales en el contenido y alcance de las convenciones y disposiciones internacionales en materia de delito cibernético. La capacitación cubría también las otras herramientas jurídicas disponibles, el manejo de las pruebas digitales, la legislación procesal relacionada con este tipo de delitos y la importancia de la cooperación jurídica internacional para su persecución y sanción. Gracias a esta iniciativa, más de 1.500 jueces, fiscales, investigadores y creadores de políticas legislativas han recibido hasta ahora formación y capacitación en 26 talleres regionales coordinados por la OEA. Los talleres han abarcado temas desde técnicas básicas de investigación y enjuiciamiento, manejo, conservación y admisibilidad de la prueba electrónica y digital, la cooperación internacional y la asistencia judicial recíproca, hasta la técnica para el desarrollo de legislación sobre Delito Cibernético con base en el Convenio del Consejo de Europa en la materia. Los contenidos de esos talleres fueron impartidos a 50 jueces y magistrados de los poderes judiciales de

[9] La Secretaría General de la OEA presta servicios de asesoría jurídica y secretaría técnica en todo lo relacionado con la preparación, celebración y seguimiento de estas reuniones; al igual que a los grupos de trabajo creados en su ámbito (Expertos en Asistencia Judicial Mutua en Materia Penal y Extradición; Grupo de Expertos Gubernamentales en Materia de Delito Cibernético; y Autoridades Responsables Además de lo anterior, la Secretaría General de la OEA brinda su apoyo al mantenimiento de la Red Hemisférica de Intercambio de Información para la Asistencia Judicial Mutua en Materia Penal y al Proyecto Piloto de Correo Electrónico Seguro para intercambio de información confidencial entre los integrantes de la Red, en ambos casos en estrecha cooperación con el Ministerio de Justicia de Canadá. Por otra parte, también está a cargo de la Secretaría General de la OEA, el mantenimiento de las páginas en Internet correspondientes a la cooperación hemisférica en el combate contra el delito cibernético y a la cooperación en políticas penitenciarias y carcelarias.

> Argentina, Paraguay, Uruguay y Chile, quienes participaron en una capacitación en cooperación jurídica contra el delito cibernético en Buenos Aires. En estos ejercicios, los participantes identificaron ejemplos de delitos informáticos que ocurren en sus países y los desafíos que existen: aprendieron sobre el Portal Interamericano en Delito Cibernético que implementó la OEA; conocieron sobre información de fuentes abiertas de datos enfocados a la investigación de los delitos informáticos, metadatos y búsquedas inversas; y recibieron entrenamiento sobre aspectos básicos de la evidencia digital, como asegurarla y garantizar la correcta preservación de la cadena de custodia. Igualmente, discutieron sobre el balance entre privacidad y seguridad y los aspectos legales de las pruebas digitales y las maneras formales e informales de obtenerlas[10] (OEA, 2016f)

Por la relevancia y auge de este tema, nunca se ha quedado estático, y en la XIX Cumbre Judicial Iberoamericana realizada en Ecuador en 2018, se señala que:

> Un aspecto importante a considerar es que en la medida que los países tengan armonizada la normativa jurídica, con el resto de la región, la misma, facilitará mayor cooperación internacional, con el fin de perseguir y castigar a los partícipes de este tipo de hechos, y consecuentemente facilitar la extradición tanto activa, como pasiva, de este tipo de conductas al margen de la Ley (Iberoamericana, Grupo E-Justicia Cumbre Judicial, 2018, p.2-3).

2.1.2. Delitos informáticos en El Salvador

[10] El taller en Buenos Aires, destinado a los países del cono sur, fue el primero de una serie que a lo largo de 2016 proyectó cubrir toda la región de Latinoamérica y el Caribe. El taller para los países centroamericanos se programó llevarlo a cabo en Costa Rica en julio; el destinado a los países caribeños se celebraría en Fort Lauderdale, (EEUU) en agosto y el orientado a la región andina se impartiría en Perú en octubre. Desde su creación, el Grupo de Trabajo en Delito Cibernético ha servido como facilitador de intercambio de información y de experiencias y para formulas recomendaciones para mejorar y garantizar la efectividad en el combate de este delito en la región. Además del combate contra el Ciberdelito, la OEA, a través del Comité Interamericano contra el Terrorismo (CICTE) y la Comisión Interamericana de Telecomunicaciones (CITEL), adelantan programas específicos para prevenir y mitigar las amenazas del delito cibernético, especialmente enfocadas en construir capacidades de seguridad entre los Estados, establecer grupos nacionales de "alerta, vigilancia y prevención", desarrollar Estrategias Nacionales sobre Seguridad Cibernética, planes de protección de infraestructura crítica y en general la seguridad del espacio cibernético

La legislación sobre el ciberdelito en el país, ha sido abordada por la comunidad académica, encontrándose interesantes artículos que permiten comprender las causas que propiciaron la aprobación de la Ley, por lo cual se cita el artículo académico escrito por Paris (2016) en el que describe que:

> “Con 70 votos de todos los partidos políticos, la Asamblea Legislativa de El Salvador aprobó la Ley Especial Contra Delitos Informáticos, Decreto No. 260, publicado en el Diario Oficial del 26 de febrero de 2016, que busca sancionar delitos cometidos por medio de las nuevas tecnologías de información y comunicación y el uso de datos almacenados y difusión de información privada (Paris, 2016a)

El autor, define como delito informático “toda aquella acción antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet” (Paris, 2016b)

Como la tecnología informática no es estática, al contrario, es muy dinámica, la legislación no se mueve al mismo ritmo que aquella, razón por la cual “existen conductas criminales por vías informáticas que aún no pueden considerarse como delito por falta de tipicidad” (Paris, 2016c).

> Una de las principales causas por las que se decidió legislar en este campo fueron situaciones de denegación de servicio, malware y troleo que se han producido en los últimos años en los sitios web de las entidades Estatales y en las empresas privada de este país. Al no contar con una tipificación establecida se producía una situación de inseguridad jurídica e impunidad. El objetivo general de esta legislación es desarrollar una normativa que proteja de manera integral el tema de la protección de identidad de las personas que acceden al mundo de la tecnología. (Paris, 2016d)
>
> Su marco de aplicación es sobre hechos punibles realizados total o parcialmente dentro del territorio salvadoreño, también se aplicará si el hecho inició fuera de dicho territorio, pero se consumó dentro de él o en los que se utilizó infraestructura tecnológica salvadoreña, por ejemplo,

redes informáticas o servidores. También se aplicará en aquellos casos en que las víctimas sean ciudadanos salvadoreños o se afecten bienes jurídicos del Estado salvadoreño. (Paris, 2016e)

Esta Ley contiene dos definiciones interesantes en materia de Protección de Datos Personales. Primero, define 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. Esta definición pareciera más acertada en su redacción que el legislador salvadoreño le dio a este mismo concepto en la Ley de Firma Electrónica que fue aprobada en el último trimestre del año 2015, sin embargo, existe una evidente contradicción entre ambas legislaciones en el tanto la Ley de Firma Electrónica define Dato Personal de Alcance Público como datos que no afectan la intimidad del titular de la misma, como los datos relativos al estado familiar de la persona entre otros, y que pueden estar contenidos en registros públicos. No obstante, en la Ley de Delitos Informáticos se incluyó una definición de Datos Personales Sensibles que los delimita como los que corresponden a una persona en lo referente al credo, religión, origen étnico, filiación o ideologías políticas, afiliación sindical, preferencias sexuales, salud física o 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. Entonces, los datos relativos al estado o situación familiar de una persona ¿Son de alcance público o sensibles? Usualmente los datos relativos a la familia son considerados sensibles, y por ende, se considera que la legislación más acertada sobre el tema, es la Ley de Delitos Informáticos. (Paris, 2016f)

2.1.3. Fortalecimiento de las capacidades en la investigación del cibercrimen en El Salvador

La Oficina de las Naciones Unidas contra la Droga y el Delito, (UNODC) para

Centroamérica y el Caribe, a través del su sitio web, publicó información sobre el fortalecimiento de las capacidades en El Salvador, en la investigación del delito cibernético, señalando que:

> En el marco de la carta de entendimiento celebrada entre UNODC y la Policía Nacional de El Salvador para el establecimiento de la Unidad de Cibercrimen dentro de la Subdirección de Investigaciones, se desarrollaron una serie de actividades de capacitación para el fortalecimiento de las capacidades de los profesionales de la justicia penal en la prevención y lucha contra el cibercrimen en El Salvador. Del 7 al 11 de Julio se desarrolló la segunda capacitación "Técnicas de Investigación en Cibercrimen" dirigida al Grupo de Delitos Informáticos, Fiscales y personal policial aspirante a conformar la futura Unidad de Cibercrimen. Con el objetivo de abordar de manera integral las necesidades de la unidad, se conformaron tres grupos: investigadores, peritos forenses y administradores. Cada uno recibió de manera especializada los conocimientos y herramientas necesarias para investigar y coordinar los casos de investigaciones en cibercrimen. Para ello se contó con la participación de Miroslav Prljevic de la Oficina de UNODC y el Dr. Joshua James de la Universidad de Corea del Sur. Anteriormente, tuvo lugar del 24 al 28 de marzo la primera capacitación en Informática Forense, que fue dirigida al mismo grupo. El objetivo del curso fue dotar a los participantes de conocimientos básicos en el área de informática forense, aportando elementos básicos sobre el manejo de la evidencia digital y el uso básico del software de recuperación de información en computadoras y teléfonos móviles, En Case. En el área técnica-científica, el curso fue impartido por el Dr. Greg Carlton de la Universidad California State Polytechnic University de los Estados Unidos de Norteamérica. Y en el área de cooperación y aspectos legales se contó con la participación de Tejal Jesrani, Experta en Justicia Criminal de la Oficina de las Naciones Unidas contra la Droga y el Delito, UNODC.

> Adicional a las capacitaciones, el Grupo de Delitos Informáticos ha contado con el acompañamiento técnico y metodológico de UNODC que permitirá sentar las bases para la creación de la Unidad de Cibercrimen de la Policía Nacional de El Salvador. (UNODC, 2020)

2.1.4. Protección de datos personales

2.1.4.1 Protección de datos personales en la dimensión internacional.

El tema de la protección de los datos personales, en El Salvador, ha sido estudiado internacionalmente antes del surgimiento de la LEDIC, por el mismo hecho del avance de la tecnología, información y comunicación que junto con éstas, generaron vacíos en detrimento de los datos personales de los individuos.

Al respecto se plantean aspectos, que revisten la importancia de protección de los datos personales, reconocidos a nivel constitucional internacionalmente:

> La necesidad de tutelar la vida privada de los individuos, rebasa la esfera estricta del derecho interno y se plantea como una exigencia de tipo internacional. En ese sentido, el derecho a la privacidad merece especial atención de parte de los organismos internacionales, así la Declaración Universal de Derechos Humanos de 1948, expresa en su Art. 12 que: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la Ley contra tales injerencias o ataques". También la Declaración Americana de los Derechos y Deberes del Hombre, de 1948, reconoce en su Art. 5 que: "Toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar". Las anteriores Declaraciones, se complementan con el Pacto Internacional de Derechos Civiles y Políticos de 1966, que en su Art. 17 manifiesta que: "1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su

honra y reputación. 2.- toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques". A los anteriores instrumentos internacionales cabe agregar, la Convención Americana sobre Derechos Humanos, o Pacto de San José de Costa Rica de 1969, la que en su Art. 11, titulado "Protección de la Honra y de la Dignidad", recoge el derecho a la privacidad.

Como se ha podido notar, dichos instrumentos no abordan directamente el derecho informático, los primeros textos internacionales referente a la protección de datos personales son, como lo señala Pérez Luño, la Resolución del Comité de Ministros del Consejo de Europa de 1973 sobre la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector privado, a la que siguió en 1974 otra Resolución de los bancos de datos en el sector público. En ellos se recomendaba a los países miembros de adopción de medidas legislativa orientadas a garantizar los siguientes principios:

a. Reconocimiento del derecho de los interesados a conocer y acceder a las informaciones que le conciernen.
b. Obligación de los bancos de datos públicos o privados de corregir la información inexacta y cancelar la obsoleta, inapropiada, irrelevante u obtenida por procedimientos ilegales.
c. Adopción de las correspondientes garantías para impedir que la difusión de datos estadísticos permitiera la identificación de sujetos individuales y para evitar la transmisión de datos a personas o entidades no autorizadas.

En septiembre de 1980, fue adoptado por el Comité de Ministros del Consejo de Europa, el Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Actos de Carácter Personal, cuyos rasgos informadores son los siguientes:

a. Trata de garantizar a cualquier persona física, sea cual fuere su nacionalidad o su residencia, el respeto a sus derechos fundamentales,

concretamente a la vida privada con respeto al tratamiento automatizado de datos de carácter personal en los sectores públicos y privados que puedan afectarle.

b. Fija como objetivo prioritario el establecimiento de límites para que los datos de carácter personal puedan ser almacenados, registrados y tratados, así como las garantías jurídicas de las personas, su defensa frente a los ficheros, automatizados públicos y privados y las excepciones que puedan lograrse.

c. Reconoce el derecho de acceso por parte de los interesados a las informaciones que les conciernen, con la posibilidad de cancelarlas o corregirlas cuando se hayan procesado indebidamente, así como la facultad de recurrir ante cualquier transgresión; y, la consagración jurídica del principio de la libre circulación de datos entre los Estados miembros. (Gutiérrez, 1994a)

2.1.4.2 En el contexto latinoamericano

Varias constituciones latinoamericanas han incluido de manera expresa disposiciones relativas a la protección de datos personales; de lo cual, Gutiérrez (1994) afirma que:

> Como ejemplo, algunas constituciones provinciales de la República de Argentina que han incluido las cláusulas relativas a la informática, derechos de acceso, rectificación y actualización: La Constitución de la Rioja (1986) establece que: La Ley limitará el uso de la informática para preservar el honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. La Constitución de San Juan (1986) prevé que todo ciudadano tiene derecho a tomar conocimiento de lo que de él conste en forma de registro y de la finalidad a que se destinan las informaciones, pudiendo exigir la rectificación de datos, así como su actualización. No se puede utilizar la informática para el tratamiento de

datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se destine para fines estadísticos no identificables; la Constitución de Córdoba en términos similares a los citados anteriormente, contempla que: toda persona tiene derecho a conocer lo que de él conste en forma de registro, la finalidad a que se destina esa información y a exigir su rectificación y actualización. Dichos datos no se pueden registrar con propósitos discriminatorios de ninguna clase ni ser proporcionados a terceros, excepto cuando tengan un interés legítimo. La ley reglamenta el uso de la informática para que no se vulneren el honor, la intimidad personal y familiar y el pleno ejercido de los derechos. También la Constitución Política de la República de Guatemala de 1987 reconoce los derechos de acceso, de corrección, rectificación y actualización al establecer en su Art. 31 Acceso a archivos y registros estatales. Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos. Posteriormente, en 1991 la Constitución de Colombia reconoció dichos derechos en los incisos 1º y 2º del Art. 15 que dice: “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. La Declaración Universal de Derechos Humanos proclamada por la Asamblea General de las Naciones Unidas en París, el 10 de diciembre de 1948, el Pacto Internacional de Derechos Civiles y Políticos que entró en vigor el 23 de marzo de 1976 y el Convenio N° 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de fecha 28 de enero de 1981, reconocen y defienden el honor, la dignidad y la protección

de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados el honor y la dignidad de la persona. (Gutiérrez, 1994b)

.

De acuerdo al Instituto de Acceso a la Información Pública (IAIP) en El Salvador, la Constitución de la República reconoce el derecho al acceso, control y protección de nuestros datos personales o mejor conocido como derecho a la autodeterminación informativa, establecido en su artículo 2; el cual sirvió de base para que la Sala de lo Constitucional reconociera la preservación de la información de las personas que se encuentra contenida en registros públicos o privados frente a la utilización arbitraria. (IAIP, 2018)

2.2. ELEMENTOS TEÓRICOS.

2.2.1. Obstáculos en la investigación de los delitos informáticos en El Salvador

Frente al panorama de la investigación de los delitos informáticos en Latinoamérica y el Caribe:

La realidad salvadoreña exhibe un escenario propio. En este contexto especifico, el ciberdelito no parece ser ni frecuente en su presencia en tribunales, ni variado en su forma de realización, lo que parece desprenderse de las mismas estadísticas de la Fiscalía General de la República, según las cuales desde el año 2016 a febrero del 2018 habían ingresado un total de 568 casos, de los cuales el 70% de los mismos se canalizaban a través de los mismos tipos penales (Revelación de datos o información, Hurto de identidad, Utilización de datos personales,

Acoso a través de TICS y comportamientos relativos a la pornografía). En otros términos, delitos que se relacionan con la intimidad o la libertad y la indemnidad sexual.

Resulta llamativa, la ausencia estadística de comportamientos de daños a sistemas o acceso sin consentimiento a los mismos, esto a pesar que la compañía de seguridad ESET para el año 2015 (ESET Security Report, Latinoamérica, 2015) reportaba que en el territorio de El Salvador un 34% de las empresas encuestadas por dicho estudio habían sido objeto de ataques a través de malware (ESET 2015, 7), sin embargo, expertos entrevistados sospechan que puede tratarse de una suerte de "cifra negra" de delitos no denunciados, ya sea por la percepción que no se trata de delitos, o bien por el desinterés de realizar el aviso una vez la intrusión o el daño ha sido contenido o reparado.

En este punto, la ONUDC hace sus propias apreciaciones sobre la base metodologías de entrevistas a diferentes actores, concluyendo que la falta de denuncias se debe a "una variedad de factores, incluida la falta de confianza del público en la capacidad de la policía de manejar un delito cibernético, el no estar enterados de la victimización y no conocer los mecanismos de denuncia, la vergüenza y pena de la víctima y los riesgos que perciben para la reputación de las corporaciones" (UNODC, 2013, 135). Para dicha oficina, la clave respecto a este fenómeno es la concientización de la población, a través de campañas y otras estrategias preventivas, un aspecto del que precisamente carece la LEDIC hasta el momento Siguiendo con los delitos que ingresan al sistema, solo en un aproximado del 10% de los casos se ejercerá la acción penal presentándose requerimiento, de estos hechos en los que se ejerce la acción penal, apenas la mitad de los mismos llegarán a la fase de presentación de Dictamen de Acusación, y las posibilidades de condena son aún más escasas. En este punto es necesario continuar investigando cuales son las salidas alternas o posibles causas de sobreseimiento que dificultan el acceso de estos delitos a la Vista Pública,

pero más importante aún, es conocer porqué tan pocos de los delitos que ingresan y conoce el ente fiscal, son requeridos ante los tribunales (10% de los ingresados), debemos recordar en este punto que la investigación de la delincuencia informática tiene dificultades añadidas en comparación al resto de delitos (transnacionalidad, horizontalidad y opacidad de las redes sociales, etc.), por lo que en caso de tratarse de estas dificultades las que impiden el procesamiento o presentación de requerimiento fiscal, debe comenzar a trabajarse en las medidas para solventar estos obstáculos.

Finalmente, debe valorarse que se trata de comportamientos que apenas comienzan a medirse, por tratarse de una ley cuya vigencia inicia en el 2016, y del que consecuentemente solo se ha visto en pleno funcionamiento durante el año 2017. Sin embargo, de continuarse con esta tendencia habría que concluirse que la LEDIC a pesar de sus muchas tipificaciones, logra escasos resultados, por los menos, si por resultados entendemos condenas[11]. (Feusier & Martínez, p. 66-67)

2.2.2. Definición de los delitos informáticos

Tomando en cuenta el avance tecnológico de la información y la comunicación, a nivel global, Feusier & Martínez, analizan la complejidad de las definiciones de los delitos informáticos, quienes, a través de su estudio de investigación y análisis, expresan lo siguiente:

Existe un consenso del cual no es difícil partir, la ciber delincuencia o el delito informático pertenece a la rama del derecho comúnmente conocida como derecho informático, es decir, aquel conjunto de normas que regulan la utilización de bienes y servicios informáticos en la sociedad (por ejemplo,

[11] Aplicación y Contenido de la Ley Especial Contra la delincuencia informática y Conexos. Concurso de Investigación Consejo Nacional de la Judicatura "Fomentando la investigación para mejorar la Administración de Justicias

el régimen jurídico del software, el derecho de las redes de transmisión de datos, los contratos electrónicos, entre otros). Más allá de este sencillo consenso, establecer límites precisos para la delincuencia informática se vuelve una labor más complicada. Sin duda alguna, lo anterior se debe al fenómeno mismo de la globalización y el acelerado desarrollo de las tecnologías de la información y comunicación (en adelante TICS), vivimos en una época en la cual las distancias y divisiones territoriales prácticamente se anulan mediante el uso de las tecnologías, afectando nuestras formas de entender el campo de lo político, jurídico, económico, y por supuesto, cultural. En este nuevo entorno en el cual el contacto con las TICS se introduce en todos los ámbitos relacionales del ser humano, será difícil diferenciar entre delitos comunes, prácticas inanes y aquellas conductas que pueden considerarse como delincuencia informática por su potencial lesivo. Sencillamente, se trata de un ámbito demasiado amplio y heterogéneo. La dificultad por alcanzar un concepto definitivo ha sido reconocida por Flores Prada, que se expresa de la problemática de la siguiente forma:

> Se debiera empezar por reconocer que no existe entre los expertos un concepto claro sobre criminalidad informática. Utilizaremos esta expresión porque es la que con mayor precisión agrupa un conjunto heterogéneo de delitos, cuya única característica común radica en la utilización de sistemas informáticos (Flores Prada, 2012, pág. 52)

La heterogeneidad es entonces el principal problema, las actuaciones criminales por medio de tecnologías informáticas pueden presentarse de múltiples formas, desde los sospechosos correos electrónicos que hemos recibido en más de alguna ocasión, y que posiblemente sean puerta de entrada para el delito de estafa, intrusismo o daños informáticos, pasando por la distribución en la red de contenidos protegidos con fines lucrativos (piratería), hasta llegar a formas más recientes y elaboradas de ciber delincuencia, como las observadas en Europa, en donde ya se ha hablado de las primeras manifestaciones de ciber-terrorismo. Por la

misma razón, Leyre Hernández termina advirtiendo la misma dificultad luego de estudiar el desarrollo del concepto de ciber criminalidad, una evolución que según la autora está influenciada por las diversas facetas que ha ido presentando este tipo de delincuencia o el desarrollo mismo de las tecnologías de la información, apareciendo en un primer momento definiciones con énfasis en el ámbito patrimonial, que con el tiempo se abrieron a otras formas de ataques a bienes jurídicos tan distintos como la intimidad, la indemnidad sexual, la propiedad intelectual, entre otros. A manera de conclusión en este punto, la referida autora parece decantarse por la idea de abandonar una definición cerrada de delito informático, y en su lugar referirse a los mismos de manera genérica, como delincuencia informática o criminalidad informática. En palabras de la misma:

> Por ello la doctrina quizás hoy mayoritaria prefiere acudir a aquellas expresiones de delincuencia informática o criminalidad informática para incluir en ellas todos 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 el mismo el propio objeto sobre el que recae la acción (Hernández Díaz, 2010, 43)

Retomando un poco las ideas expresadas por Flores Prada, lo que parecería ser el elemento medular de esta forma comisiva es el medio utilizado para la comisión del ilícito, estamos en presencia de delitos que esencialmente se cometen a través de tecnologías de la información y comunicación, una conclusión en la que también parece coincidir Arrocena, que al momento de entender estos delitos expresa lo siguiente:

> El delito informático o ciber delito es el injusto determinado en sus elementos por el tipo de la ley penal, conminado con pena y por el que el autor merece un reproche de culpabilidad, que, utilizando a los sistemas informáticos como medio comisivo o teniendo a aquéllos, en parte o en todo, como su objeto, se vinculan con el tratamiento automático de datos (Arrocena, 2011, 950)

Se trata también, de una definición similar a la relacionada en el actual decreto de Ley Especial contra los Delitos Informáticos y Conexos, que en su artículo 3, literal a), dedicado a realizar Definiciones, entiende por delito informático cuando se haga uso de las Tecnologías de la Información y la Comunicación, teniendo por objeto la realización de la conducta típica y antijurídica para la obtención, manipulación o perjuicio de la información.

Como se puede observar, la utilización medial de las TICS constituye el elemento central de la definición, aunque el legislador le adicione un segundo elemento típico también fundamental, este de carácter subjetivo especial como lo es la intención o finalidad de realizar una conducta típica para obtener, manipular o perjudicar información, lo que en principio generaría dudas si pueden considerarse típicos comportamientos aparentemente inservibles, podemos imaginar el supuesto de un hacker que ingresa a un sistema evadiendo la seguridad del mismo, sin hacer ningún tipo de daño ni apoderándose de información alguna, sino por el simple deseo de demostrar su pericia y habilidad a terceros. Estas dudas aumentan, cuando leemos los primeros tipos penales que regula la LEDIC, por ejemplo, el tipo penal de Acceso Indebido a Sistemas Informáticos (art. 4 decreto de LEDIC), mismo que se realiza cuando intencionalmente y sin autorización o excediendo la que se le hubiere concedido, acceda, intercepte o utilice parcial o totalmente un sistema informático que utilice las Tecnologías de la Información o la Comunicación. Como se puede observar, el comportamiento en cuestión solo requiere acceder a un sistema, independientemente de la finalidad o deseo de obtener, manipular o perjudicar información, dejando al intérprete la labor de determinar si la definición de delito informático apuntada en el párrafo que antecede, es una definición incorrectamente formulada, o sencillamente el referido tipo penal es una suerte de norma penal de peligro abstracto dentro de una ley cuyo catálogo de comportamientos tienen un bien jurídico de por sí bastante difícil de precisar. En suma, podemos decir que tanto la doctrina, como el decreto de LEDIC, se

decantan por una definición amplia de delito informático, entendiendo por el mismo aquel acto típico que se realiza mediante la utilización de una tecnología de la información o comunicación, adicionándose en el caso específico de nuestro decreto de ley, un elemento subjetivo especial que llamativamente no se presenta en casi ninguna de las especies criminales reguladas en el mismo, y que incluso, desdibujan o pierden sentido en otros tipos penales, como lo pueden ser los relacionados a la transferencia de contenidos pornográficos de menores o hacia éstos. (Feusier & Martínez, p. 4-7)

2.2.3. Definición de delitos informáticos más relevantes que se regularon con la LEDIC

De acuerdo al autor citado en el numeral 2.1.2, en su artículo sobre La Nueva Ley de Delitos Informáticos de El Salvador, se definen los delitos más relevantes que se regularon con la Ley Especial contra Delitos Informáticos y Conexos (LEDIC):

- **Acceso indebido a sistemas informáticos:** que se podría configurar por ejemplo accediendo sin permiso al whatsapp de su pareja.

- **Daños a sistemas informáticos:** que se sancionan incluso de forma culposa en casos de imprudencia, negligencia, impericia o inobservancia de las normas establecidas, por ejemplo, un empleado que instala software malicioso sin autorización en contradicción con las políticas de seguridad informática de la empresa.

- **Posesión de equipos o prestación de servicios para la vulneración de la seguridad**: es un tipo penal curioso por cuanto sanciona la mera tenencia con fines de comercialización de estos equipos.

- **Acoso sexual tecnológico**: Se sanciona una conducta sexual indeseada por su

receptor que implique frases, señas u otras conductas inequívocas de carácter sexual.

- **Estafa y el fraude informático:** La diferencia entre ambos tipos penales es muy sutil y parece que puede complicar su aplicación en cuanto a tipicidad de las conductas. Pareciera que la diferencia radica en que en el fraude informático el hecho ilícito principal es el uso indebido de la tecnología, mientras que, en la estafa, la tecnología es sólo la herramienta mediante la cual se comete el delito. Es decir, por ejemplo, la alimentación con órdenes de compra falsas de un sistema de compras de una empresa sería una estafa informática, mientras que el hackeo de dicho sistema para procurar un pago en una cuenta bancaria distinta de la registrada sería un fraude informático.

- **Utilización de Datos Personales:** Se sanciona el mero uso sin autorización de datos personales por medio de sistemas informáticos, sin diferenciar el tipo de datos personales que sean utilizados, lo cual pareciera excesivo, tomando en consideración que la Ley define Datos Personales Sensibles, que son los que entendemos revisten un mayor interés en su protección.

- **Delitos informáticos contra menores de edad:** Se regula con gran detalle situaciones de vulnerabilidad de menores de edad, tales como pornografía, corrupción y acoso.

- **Acciones tipo revenge porn:** Se sanciona la revelación indebida de datos o información de carácter personal cuando sin consentimiento se difunda información o datos, siendo un agravante en la pena que se trate de imágenes, videos, textos o audios que constituyan material sexual explícito.

(Paris, 2016g)

2.2.4. Delito De Revelación Indebida De Datos O Información De Carácter Personal

2.2.4.1 Tipificación del delito de revelación indebida de datos o información de carácter personal.

2.2.4.1.1 En Latinoamérica

De acuerdo a la Cumbre Judicial Iberoamericana, edición XIX, celebrada en Ecuador, en abril de 2018, el tema de interés abordado fue la ciberdelincuencia, generando como resultado un importante compendio normativo sobre esa, y para el caso del presente trabajo, se destaca la tipificación del Delito de Revelación Indebida de Datos o Información de Carácter Personal, pero no como tal, sino que en los diversos países de Latinoamérica, se tipifica de forma diferente, pero siempre siendo congruente con el delito en estudio. Es así como se presenta la siguiente información breve pero precisa:

2.2.4.1.1.1 Colombia

> Artículo: 269F
>
> Norma: Código Penal (adicionado por Art. 1°Ley 1273 de 2009) Tipo Penal: Violación de Datos Personales.
>
> Descripción: El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales cometidos en ficheros, archivos, base de datos o medios semejantes, incurrirá en pena de presión de cuarenta y ocho (48) a noventa y seis (96) meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes. (Iberoamericana, Grupo E-Justicia Cumbre Judicial, 2018, p.125)

2.2.4.1.1.2 Costa Rica

Artículo: 196 bis

Norma: Código Penal (Adicionado mediante Ley 8148 del 2001 y posteriormente reformado por Ley N° 9135 del 2013)

Tipo Penal: Violación de Datos Personales

Descripción: Será sancionado con pena de prisión de uno a tres año quien en beneficio propio o de un tercero, con peligro o daños para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, trasmite, publica, difunda, recopile, utilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fue recolectado o de un tratamiento de no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónico, ópticos o magnéticos.

La pena será de dos a cuatro años de prisión, cuando las conductas descritas en esta norma:

a. Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengas acceso a dicho sistema o red, o a los contadores electrónicos, ópticos o magnéticos.
b. La información vulnerada corresponda a un menor de edad o incapaz.
c. Las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona.
d. No constituye delito la publicación, difusión o transmisión de información de interés público, documentos públicos, datos contenidos en registros públicos o base de datos públicos de acceso irrestrictivos cuando se haya tenido acceso de conformidad con los procedimientos y limitaciones de ley.

Tampoco constituye delito la recopilación, copia y uso por parte de las entidades financieras supervisadas por la Sugef de la información y datos contenidos en bases de datos de origen legítimo de conformidad con los procedimientos y limitaciones de ley. (Iberoamericana, Grupo E-Justicia Cumbre Judicial, 2018, p.125-128)

2.2.4.1.1.3 El Salvador

Artículo: 26

Norma: Ley Especial Contra Delitos Informáticos y Conexos.

Tipo Penal: Revelación Indebida de Datos o Información de Carácter Personal.

Descripción: El que sin el consentimiento del titular de la información de carácter privado y personal revele, difunda o ceda en todo o en parte, dicha información o datos a los que se refiere el presente artículo, sean estos en imágenes, videos, texto, audio u otros, obtenidos por algunos de los medios indicados en artículos precedentes, será sancionado con prisión de tres a cinco años.

Si alguna de las conductas descritas en el inciso anterior, se hubiese realizado con ánimo de lucro, la comisión de otro delito o se difunda material sexual explícito en perjuicio de un tercero, será sancionado con prisión de cuatro a ocho años. Se impondrá el límite máximo de las penas del inciso anterior, aumentada hasta en una tercera parte, si alguna de las conductas descritas en el inciso primero del presente artículo, recae sobre datos personales, confidenciales o sensible definidos en la Ley de Acceso de Información Pública. (Iberoamericana, Grupo E-Justicia Cumbre Judicial, 2018, p. 128)

2.2.4.1.1.4 Ecuador

Artículo: 178

Norma: Código Orgánico

Integral Penal Tipo Penal: Violación

a la intimidad.

Descripción: Persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas por otras personas por cualquier medio, será sancionado con una pena privativa de libertad de uno a tres años. No son aplicables estas normas para las personas que divulguen grabaciones de audio y video en las que interviene personalmente, ni cuando se trate de información pública de acuerdo con lo previsto en la ley. (Iberoamericana, Grupo E-Justicia Cumbre Judicial, 2018, pág. 128)

2.2.4.1.1.5 Nicaragua

Artículo: 192

Norma: Ley 641 Código Penal. Reformado por el Art. 58 de la Ley 779 Ley Integral contra la Violencia hacia las mujeres y de Reformas a la Ley 641 Código Penal

Tipo Penal: Propalación.

Descripción: Quien, hallándose legítimamente en posesión de una comunicación, de documentos o grabaciones de carácter privado, lo haga público sin la debida autorización, aunque le hayan sido dirigidos, será penado de sesenta a ciento días multa. Adición Si las grabaciones, imágenes, comunicaciones o documentos hechos públicos son de contenido sexual o eróticos, aunque hayan sido obtenidos con el consentimiento, la pena será de dos a tres años de prisión. Cuando se

trate de documentos divulgados por internet, el Juez competente a petición del Ministerio Público o quien esté ejerciendo la acción penal, ordenará el retiro inmediato de los documentos divulgados. (Iberoamericana, Grupo E-Justicia Cumbre Judicial, 2018, p.129)

2.2.4.1.1.6 República Dominicana

Artículo: 6

Norma: Ley N° 53-07, sobre Crímenes y Delitos de Alta Tecnología

Tipo Penal: Uso de Datos por Acceso Ilícito.

Descripción: El hecho de acceder a un sistema electrónico, informático, telemático o de telecomunicaciones o a sus componentes, utilizando o no una identidad ajena, o excediendo una autorización, se sancionará con las penas de tres meses a un año de prisión y multas desde una vez hasta doscientas veces el salario mínimo. Párrafo I.- Uso de Datos por Acceso Ilícito. Cuando dicho acceso ilícito resulte la persecución o la modificación de datos contenidos en el sistema, o indebidamente se revelen o se difundan datos confidenciales contenidos en el sistema accesado, las penas se elevarán desde un año hasta tres años de prisión y multas desde dos hasta cuatrocientas veces el salario mínimo. (Iberoamericana, Grupo E-Justicia Cumbre Judicial, 2018, p.131-132)

2.2.4.1.2 En El Salvador

La Oficina de las Naciones Unidas contra la Droga y el Delito, para Centroamérica y el Caribe, UNODC ROCPAN, a través de la Escuela de Capacitación Fiscal, realizaron un 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, encontrándose tipificado en el artículo 26:

Revelación Indebida de Datos o Información de Carácter Personal

Art. 26.- El que sin el consentimiento del titular de la información de carácter privado y personal revele, difunda o ceda en todo o en parte, dicha información o datos a los que se refiere el presente artículo, sean éstos en imágenes, video, texto, audio u otros, obtenidos por alguno de los medios indicados en los artículos precedentes, será sancionado con prisión de tres a cinco años.

Si alguna de las conductas descritas en el inciso anterior, se hubiese realizado con ánimo de lucro, la comisión de otro delito o se difunda material sexual explícito en perjuicio de un tercero, será sancionado con prisión de cuatro a ocho años.

Se impondrá el límite máximo de la pena del inciso anterior, aumentado hasta en una tercera parte, si alguna de las conductas descritas en el inciso primero del presente artículo, recae sobre datos personales confidenciales o sensibles definidos en la Ley de Acceso a la Información Pública.

a) Bien jurídico.

El legislador salvadoreño colocó este tipo penal en el capítulo que ha denominado Delitos Informáticos relacionados con el contenido de los datos, y es de los tipos penales de la LEDIC que menciona en su redacción al contenido de la información (los datos informáticos) como objeto de protección, por lo que podemos señalar que el bien jurídico tutelado en consecuencia, coincide con lo que hemos afirmado en los comentarios al art.4 de la LEDIC, en el sentido que se puede comenzar a sostener que estamos en presencia de un valor social que necesita la protección del derecho y en particular del derecho penal, que se ha categorizado como la integridad de los sistemas y datos informáticos.

No obstante, lo anterior, en virtud que además se sanciona la difusión o cesión de información de carácter privada y personal es posible vincularlo con el derecho a la intimidad, materializado en el contenido de los datos

informáticos, por lo que se puede hablar de un tipo penal pluriofensivo, entre el derecho a la intimidad y la mencionada integridad de sistemas y datos informáticos. (UNODC ROPAN, 2018, p. 92)

b) Elementos objetivos

b.1) Sujeto activo.

Común: En virtud de la formulación utilizada por el legislador, consistente en “El que sin el consentimiento”, podemos concluir que se trata de un delito común, en el cual el sujeto activo no debe contar con ninguna cualidad o calidad especial, por lo que puede ser realizado por cualquier persona natural.

b.2) Sujeto pasivo.

Común: Puede ser sujeto pasivo cualquier persona natural o jurídica titular de la información de carácter privada y personal.

b.3) Conducta típica.

La parte objetiva de la conducta típica comprende el que “sin el consentimiento del titular de la información de carácter privado y personal revele, difunda o ceda en todo o en parte, dicha información o datos a los que se refiere el presente artículo, sean éstos en imágenes, video, texto, audio u otros, obtenidos por alguno de los medios indicados en los artículos precedentes.

Los verbos rectores del tipo penal están conformados por revelar, difundir o ceder en todo o en parte, lo que indica que son conductas alternativas, es decir que no se deben cumplir todas para consumar el delito, sino que basta con la realización de una de ellas. Revelar, como ya se ha señalado es descubrir o manifestar lo ignorado o secreto; por su parte difundir, es - **3**. tr. Propagar o divulgar conocimientos, noticias, actitudes, costumbres, modas, etc.”; y ceder, es “**1**.tr. Dar, transferir o traspasar a alguien una cosa, acción o derecho”.

Todas las acciones recaen sobre la información de carácter privado y

personal, al respecto la LEDIC, no dispone una definición de tales conceptos en su conjunto, sin embargo, cuando define datos personales y datos personales sensibles, hace acopio de información privada y de que esta se refiere a información de las personas, de tal manera que podemos considerar que se trata de vocablos que en conjunto han sido utilizado como sinónimos, por lo que, los consideramos elementos normativos y a esas definiciones remitimos.

Art. 3.- Para los efectos de la presente Ley, se entenderá por:

(…) 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;(…)".
Sobre el contenido de la información, el tipo penal además determina los medios sobre los cuales esta se puede haber soportado, al señalar "sean éstos en imágenes, video, texto, audio u otros, vocablos que se explican por sí mismos, salvo la cláusula de apertura u otros, que permitiría incluir algún otro medio de soporte.
El tipo señala además que se trata de la revelación, difusión o cesión de información sin el consentimiento del titular, de tal manera que contar con el consentimiento de este, produce la atipicidad de la conducta.

Finalmente, el tipo hace alusión a que la información objeto de la revelación, difusión o cesión, debe haber sido asequible para el sujeto activo por alguno de los medios indicados en los artículos precedentes, por lo cual a esos comentarios remitimos, pero que abre la posibilidad de discutir si en esos casos nos encontramos en presencia de un concurso

aparente de leyes o alguna de las figuras concursales que regula el CP; sin embargo, también cabe acotar, que comete delito tanto el que accede a la información personal y sensible por alguno de los medios señalados en los artículos precedentes y luego la difunde -aquí es donde se puede determinar la clase de concurso-, pero también, quien sin intervenir en los otros delitos, accede a la información y sin consentimiento del titular la revela, difunde o cede.

Piense por ejemplo en el caso que A, realizando acciones de vulneración de medidas de seguridad específicas de un sistema, programa o datos informáticos, accede a información personal y sensible de B, y luego, por un precio -que desde el inicio fue su intención: ánimo de lucro-, se la cede a C, quien es quien la revela en una cuenta de redes sociales anónima. La conducta de A, podría ser calificada como Obtención y Transferencia de Información de Carácter Confidencial, sancionada en el art. 25 de la LEDIC, mientras que la realizada por C, que no intervino en la primera conducta, se puede calificar conforme al artículo que se comenta.

b.4) Consumación y tentativa.

Por los elementos objetivos del tipo penal, señalados anteriormente, y principalmente por los verbos rectores consideramos que se trata de un delito de mera actividad, pues solo señala una mera acción, sin resultado separable espacio temporalmente de la conducta, de tal manera que el delito se consuma con la mera difusión, revelación o cesión de la información.

b.5) Conductas agravadas.

En los incisos segundo y tercero del art. 26 de la LEDIC, se consideran agravadas respecto al inciso primero, las conductas realizadas por el autor, de la siguiente forma:
Si alguna de las conductas descritas en el inciso anterior, se hubiese realizado con ánimo de lucro, la comisión de otro delito o se difunda

material sexual explícito en perjuicio de un tercero, será sancionado con prisión de cuatro a ocho años.
Se impondrá el límite máximo de la pena del inciso anterior, aumentado hasta en una tercera parte, si alguna de las conductas descritas en el inciso primero del presente artículo, recae sobre datos personales confidenciales o sensibles definidos en la Ley de Acceso a la Información Pública.

En el caso del inciso segundo, si el sujeto activo actúo con ánimo de lucro, es decir de obtener un beneficio patrimonial, si lo hizo con la intención de cometer otro delito, que puede estar sancionado en la misma LEDIC u otras leyes; y si se refiere a material sexual explícito en perjuicio de un tercero, en este último caso hay que valorar las relaciones concursales que puedan existir, en el caso que la persona afectada sea mujer, pues en los arts. 50 y 51 de la LEIV, se sancionan conductas de la misma naturaleza, así:

"Artículo 50.- Difusión Ilegal de Información

Quien publicare, compartiere, enviare o distribuyere información personal que dañe el honor, la intimidad personal y familiar, y la propia imagen de la mujer sin su consentimiento, será sancionado con pena de uno a tres años.

Artículo 51.- Difusión de Pornografía
Quien publicare, compartiere, enviare o distribuyere material pornográfico por cualquier medio informático o electrónico en el que se utilice la imagen o identidad de la mujer sin su consentimiento, será sancionado con pena de tres a cinco años."

En relación al inciso tercero del art. 26 de la LEDIC, la agravante se refiere a sí la información revelada se refiere a datos personales de carácter confidencial o sensible, tal como se encuentran definidos en la LAIP, vale hacer notar que esas definiciones son iguales en esa norma jurídica (art. 6 letras a y b) y en las definiciones del art. 3 letras m) y de la LEDIC, y

> adicionalmente como hemos señalado, en el inciso primero al carecer de definición de información privada y personal, recurrimos a los mismos conceptos, por lo que a nuestro juicio el legislador está aplicando una agravante sobre una conducta que ya forma parte del inciso primero, con lo cual recurrir a tal agravante puede conducir a una vulneración del Principio Nebis in ídem, es decir a la prohibición de la sanción penal múltiple, con lo cual consideramos que no debería ser aplicable este inciso. (UNODC ROPAN, 2018, p.92-95)

c) **Elementos subjetivos**.

c.1) Dolo.

El elemento subjetivo se determina en el dolo, es decir en el conocimiento y la voluntad de realizar el tipo.

c.2) El ánimo de lucro

Como pudo observarse, en el inciso segundo se contempla una agravante en virtud de este ánimo especial, entendido como la pretensión del sujeto activo en el sentido de obtener como resultado de su acción un beneficio patrimonial. (UNODC ROPAN, 2018, p. 95)

Por otra parte, es oportuno mencionar que, en el país, el Derecho a la autoderminación juega un papel muy importante, en relación a la utilización de la información pública y privada enfocada a la divulgación de información personal. De esto hace mención la Sentencia de Inconstitucionalidad 35-2016 de la Sala de lo Constitucional de la Corte Suprema de Justicia, en la cual se sustenta lo siguiente:

> Derecho a la autodeterminación informativa, la que se considera como una derivación del valor constitucional de la seguridad jurídica en el Art.2 el cual tiene por objeto preservar la observación individual que se encuentra contenida en el registro público o privado frente a su utilización arbitraria, con independencia de si estos afectan la esfera íntima de la persona. En ese sentido el derecho en estudio presupone la capacidad de las personas para decidir y controlar las actividades relacionadas con sus datos personales –individuales y familiares- ante su posible uso

> indiscriminado, arbitrario o sin certeza sobre sus fines y límites (Inconstitucionalidad, Ley de Partidos Políticos, 2017a)

En la sentencia del 20-X-2014, Amparo 142-2012, se encontraron dos facetas, exponiendo que:

> En la faceta material el derecho a la autodeterminación informativa pretende satisfacer la necesidad de las personas de preservar su identidad ante la revelación y el uso de datos que le conciernen, protegiéndolos frente a la ilimitada capacidad de archivarlos, relacionarlos y transmitirlos que supone el desarrollo actual y futuro inmediato de la información. Según dicha faceta o dimensión material, toda persona adquiere una situación que le permite definir la intensidad con que desea que se conozcan y circulen tanto su identidad como otras circunstancias y datos personales, combatir las inexactitudes o falsedades que la alteren y defenderse de cualquier utilización abusiva, arbitraria, desleal o ilegal que pretenda hacerse de esos datos. Aunado a lo anterior, se precisó que la autodeterminación informativa también posee una fase instrumental, en la cual el derecho conlleva al control de la información personal sistematizada o contenida en bancos de datos informáticos o ficheros, particularmente a través de medidas estatales, de tipo organizativo-institucionales y procedimental, que son indispensables para la protección del ámbito material del derecho asegurado constitucionalmente. Así, la dimensión instrumental de tal derecho no supone solamente una barrera al legislador de producir normas contrarias al mismo (deber de abstención), sino que además envuelve la posibilidad de un control efectivo por medio de procedimientos institucionales y del ejercicio de la potestad sancionadora administrativa en caso de infracciones al derecho en sentido material (Inconstitucionalidad, Ley de Partidos Políticos, 2017b)
>
> El derecho a la autodeterminación informativa, que comparta diferentes facultades de controlar sobre el uso de la información personal que le atañe, tanto en su recolección como en su tratamiento, conservación y

transmisión, no es ilimitado. Las personas individuales y colectivas carecen de derechos fundamentales absolutos sobre sus datos. Esta es la razón por la que el individuo debe de tener límites a ese derecho, por razón de un interés general. Del mismo modo, se acató que las restricciones o limitaciones pueden encontrarse justificadas en la finalidad que persigue la recolección y administración de los datos personales, la cual debe de ser legítima (constitucional o legal), explícita y determinada. Para ello el legislador debe tener en cuenta no solo el principio de proporcionalidad, sino también el derecho general del ciudadano a la libertad frente al Estado, que solo puede ser restringida por el poder público cuando se indispensable para la protección del interés general (Inconstitucionalidad, Ley de Partidos Políticos, 2017c)

En perspectiva con lo antes expuesto, cuando la información pública contiene datos personales de alguna o algunas personas, hay un ejercicio simultáneo de ambos derechos: el solicitante invoca su derecho de acceso a la información y el titular de la información requerida exige que sus datos sean protegidos frente a su acceso y uso por parte de terceros. Tal como se señaló anteriormente, corresponde al legislador delimitar el ejercicio de ambos derechos fundamentales, para lo cual puede regular los parámetros y procedimientos a observar en orden a evitar la intervención injustificada de un derecho respecto del otro (Inconstitucionalidad, Ley de Partidos Políticos, 2017d)

2.3 DEFINICIÓN Y OPERACIONALIZACIÓN DE TÉRMINOS BÁSICOS

2.3.1. Delito informático o Ciberdelito.

De acuerdo Mauricio Paris (Paris, 2016h) un delito informático o ciber delito es toda aquella acción antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito.

2.3.2. 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 (LEDIC, 2016a)

En la sentencia del 8-III-2013, Inc.58-2007, se acotó que

> Los datos personales son signos y distintivos que aportan información numérica, alfabética, gráfica, acústica o de cualquier otro de persona física o jurídica identificadas o identificables, los cuales permiten determinar, directa o indirectamente, su identidad física, filosófica, psíquica, cultural o social. Dentro de esta categoría se distinguen un conjunto de datos que revelan una esfera más privada del sujeto, que puede decidir reservar para sí o algunas personas pues su publicidad o uso por terceros podría causar una invasión desproporcionada en la intimidad personal, razón por la cual se le denomina dato sensible (Inconstitucionalidad, Ley de Partidos Políticos, 2017e)

2.3.3. 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

(LEDIC, 2016b)

De acuerdo a la Sentencia del 8-III-2013, Inc.58-200758-2007, se puntualizó que

> los datos personales sensibles se refieren a la información que aluden a la pertenencia racial o étnica de un individuo, a sus preferencias políticas, su estado individual de salud, sus convicciones religiosas, filosóficas o morales, su intimidad u orientación sexual y, en general, a toda información que fomente prejuicios y discriminaciones, o afecten la dignidad, la privacidad, la intimidad doméstica y la imagen privada de personas o familias. Por ello, se enfatizó que los titulares de estos datos no están obligados a proveerlos a la Administración, a menos que haya un conocimiento informado, exista un mandato legal o una razón de interés público que lo motive y, en ese último supuesto, dichas entidades tendrán la responsabilidad de regular y proteger su acceso por parte de terceros. (Inconstitucionalidad, Ley de Partidos Políticos, 2017f)

2.3.4. Tecnologías de la Información y la Comunicación (TICs)

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 (LEDIC, 2016c)

2.3.5. Revelación Indebida de Datos o Información de Carácter Personal

El que sin el consentimiento del titular de la información de carácter privado y personal revele, difunda o ceda en todo o en parte, dicha información o datos a los que se refiere el presente artículo, sean éstos en imágenes, video, texto, audio u otros, obtenidos por alguno de los medios indicados en los artículos precedentes, será sancionado con prisión de tres a cinco años.

Si alguna de las conductas descritas en el inciso anterior, se hubiese realizado con ánimo de lucro, la comisión de otro delito o se difunda material sexual explícito en perjuicio

de un tercero, será sancionado con prisión de cuatro a ocho años.

Se impondrá el límite máximo de la pena del inciso anterior, aumentado hasta en una tercera parte, si alguna de las conductas descritas en el inciso primero del presente artículo, recae sobre datos personales confidenciales o sensibles definidos en la Ley de Acceso a la Información Pública (LEDIC, 2016d)

Constituye un cúmulo de información relativa a una persona física, identificada o identificable. Es de suma importancia el establecimiento de mecanismos y medidas de protección que garanticen que nuestros datos personales no sean sujetos de manipulación, comercialización u otra finalidad distinta para la cual fueron generados o regulados. Que solo pueden ser utilizados bajo nuestro consentimiento y para los fines lícitos para los cuales autoricemos su uso, y en caso que suceda lo contrario, podamos defendernos.

La protección debemos entenderla como el conjunto de medidas que busca proteger los datos personales o información, de manera que éstos no puedan ser tratados, elaborados y convertidos en información pública, sino más bien que sean manipulados exclusivamente para los fines y por las instituciones autorizadas para ello, teniendo el ciudadano titular de los datos pleno conocimiento de ello.

Bien jurídico lesionado

Corresponde al almacenamiento, procesamiento, análisis, vinculación con la casi totalidad de las dimensiones de la vida en sociedad (la banca, los seguros, el comercio, los transportes, la educación, la bolsa, el tráfico aéreo y terrestre, la salud, las administraciones públicas, las entidades privadas, entre otros), el desarrollo de las tecnologías de la información y comunicación a efecto de potenciar y maximizar todo lo anterior, y adicionalmente “sobresale sin duda la configuración anárquica y supranacional de la red (internet) como un espacio transfronterizo, que carece de centro de decisión” (Flores Prada, 2012,p.49) y en consecuencia, las posibilidades de anonimia que tales desarrollos tecnológicos permiten.

2.4 PREGUNTAS DE INVESTIGACIÓN E HIPÓTESIS

Al investigar la implementación de la LEDIC en la ciudad de San Miguel, los obstáculos se agravan, ya que la PNC y la FGR no cuentan con una unidad especializada. La PNC únicamente se limita a tomar denuncias y remitirlas a la FGR y ésta a su vez la remite a San Salvador, lo cual genera un evidente retraso en la investigación, persecución y judicialización de este tipo de delitos, generando en consecuencia, una inseguridad e impunidad jurídica.

Lo cual genera en la población salvadoreña, específicamente en el área de San Miguel, una incertidumbre respecto a las soluciones para este tipo de delitos, lo cual conlleva al desinterés de su participación en la denuncias y seguimiento en los tribunales, tomando como base los pocos delitos que han sido denunciados y no se les ha dado una debida diligencia, para poder dar a la población una seguridad jurídica adecuada y romper con el paradigma de impunidad e incertidumbre, al no tener claridad.

De acuerdo a lo anterior, en la ciudad de San Miguel, es evidente la deficiencia en la investigación de la Policía Nacional Civil y Fiscalía General de la Republica, respecto al Delito de Revelación Indebida de Datos o Información de Carácter Personal; lo que genera una clara impunidad frente a la población que se atreve a denunciar este tipo de delito; de ello puede inferirse que, muy probablemente, no se cuenta con los recursos necesarios como herramientas idóneas y formación especializada al personal, para hacerle frente a los desafíos que exige esta realidad en la investigación de este delito.

- En la Fiscalía General de La República y en la Policía Nacional Civil, con sedes en la ciudad, municipio y departamento de San Miguel, no existen unidades especializadas en el Ciberdelito.
- Las Unidades especializadas en Ciberdelito se encuentran centralizadas en San Salvador.

- ¿Por qué el delito de revelación indebida de datos o información de carácter personal, el más denunciado?

- ¿Cuántas denuncias por el delito de revelación indebida de datos o información de carácter personal, están siendo investigados?

CAPÍTULO III: METODOLOGÍA DE LA INVESTIGACIÓN

3.1 TIPO DE ESTUDIO Y ESTRATEGIA METODOLÓGICA

El tipo de estudio que se utilizará es el exploratorio, con la finalidad realizar la formulación de un problema con la finalidad de posibilitar una investigación más precisa para desarrollar una hipótesis.

Por lo tanto, el tipo de investigación se propone de campo y de naturaleza jurídica, ya que se intenta comprobar e identificar la falta de herramientas tecnológicas y capacidad técnica y jurídica que tienen los funcionarios del Departamento de Investigaciones de la PNC, Unidad Especializada de la Fiscalía General de la República; lo cual determina su nivel de eficacia en cuanto de minimizar los niveles de impunidad del delito *Revelación indebida de datos o información de carácter personal.*

La estrategia metodológica que se realizará se detalla a continuación:

- Trabajo de campo y documental: recolección de datos estadísticos, encuestas, entrevistas y cuestionarios a los investigadores de la Policía Nacional Civil, fiscales de la ciudad de San Miguel.
- Requerimientos de información a la Policía Nacional Civil y Fiscalía General de la República de la ciudad de San Miguel, sobre estadística de los delitos informáticos.
- Consulta de la doctrina sobre la investigación de los delitos informáticos: libros y

revistas especializadas.

3.2 TÉCNICA E INSTRUMENTOS

Cuestionarios y entrevistas individuales a las unidades de la FGR y PNC, revisión de literatura como libros, documentales, páginas web, datos estadísticos, doctrina definiciones, conceptos, diferentes teorías relacionadas con la temática, así como jurisprudencia nacional e internacional, al igual que resoluciones de juzgados, cámara y sala.

3.3 ETAPAS DE LA INVESTIGACIÓN

Etapa 1:

Identificar los límites que tienen la Policía Nacional Civil y la Fiscalía General de la República, de la ciudad de San Miguel para la implementación eficaz de la Ley Especial contra los delitos informáticos y conexos, a través de investigación en campo en las mencionadas instituciones, mediante entrevistas, revisión de datos estadísticos, artículos, tesis, monografías, revistas e información de organismos internacionales que han acompañado la temática.

Etapa II

Investigar cuáles son las técnicas y herramientas en la FGR y PNC para la investigación del delito de revelación indebida de datos o información de carácter personal.

Asimismo, conocer cuántas denuncias, cuántos casos son investigados, cuántos condenados y cuántos absueltos en la ciudad de San Miguel.

Etapa III

Conocer el tipo de formación, capacitación, número de personal, y las edades entre las cuales oscilan, así como también qué tipo de profesión tienen, las herramientas (hardware y software) ¿son las adecuadas de acuerdo al avance de la tecnología?

3.4 PROCEDIMIENTO DE ANÁLISIS

Una vez recopilada la información, se consolidará a través de resúmenes, tablas y la transcripción de las entrevistas.

CAPÍTULO IV: HALLAZGOS EN LA INVESTIGACIÓN

4.1. PRESENTACION Y DISCUSIÓN DE RESULTADOS.

4.1.1 Aspectos preliminares sobre las conclusiones.

Los hallazgos encontrados mediante la investigación desarrollada en base al protocolo establecido por la Universidad, en el contexto del trabajo final del estudio de Maestría en Derecho Penal, en el tema “Límites a la Implementación de la Ley Especial de Delitos Informáticos y Conexos, en el Delito de Revelación Indebida de Datos o Información de Carácter Personal”, se presentan a continuación.

Inicialmente, se identificaron las Instituciones: Policía Nacional Civil y Fiscalía General de la República; luego, los actores que forman parte de las referidas instituciones y que son fuentes directas, certificadas y vinculadas a la temática de la investigación del “Delito de Revelación Indebida de Datos o Información de Carácter Personal” para lo cual se utilizó la herramienta de la entrevista, como el medio para obtener la información.

En la etapa de realización de la fase de campo del proyecto, se cumplimentó lo planificado para entrevistar a las personas idóneas antes relacionadas. Después de obtener la información, se procedió a transcribirla y analizarla, lo que permitió identificar y dar respuesta a los objetivos planteados. Por cada institución, se elaboraron dos cuadros para permitir mayor facilidad al momento de procesar la información, estableciendo dos categorías con sus respectivos complementos, con la finalidad de cotejar las respuestas obtenidas, las cuales fueron teorizadas de acuerdo a la construcción de la problemática.

Durante la investigación, la información obtenida fue procesada mediante la técnica e instrumentos cualitativos, para lo cual se hizo uso de entrevistas y análisis documental proporcionados por las instituciones en relación.

En congruencia a lo anterior, se muestra el desarrollo y la información obtenida a

través de dichos instrumentos, los cuales metodológicamente, se abordan en el orden que sigue a continuación:

Presentación de las entrevistas

a) Presentación de análisis documental del contenido esencial de las instituciones

4.1.2 Presentación de entrevistas mediante categorías metodológicas.

Se presenta la investigación de manera sistematizada, procediendo a plasmar la información obtenida en la cual se basará para elaborar las conclusiones de este proyecto.

Paso 1. Extracción de la información obtenida: se transcribe en cuadros codificados (información general y entrevistas) el contenido de la investigación de campo realizada a personas certificadas en cada una de las instituciones, tales respuestas fueron emitidas de acuerdo al formato elaborado, conforme a la investigación del proyecto, lo que permitió tabularlo.

Paso 2. Las respuestas obtenidas por cada instrumento, se codifican de acuerdo a cada categoría, para poder realizar el análisis del contenido de cada investigación.

Paso 3. El investigador realiza un análisis de las respuestas generadas por las instituciones/sujeto, relacionándolas con los objetivos e hipótesis planteados en el proyecto de investigación.

a) Policía Nacional Civil, sede San Miguel

i. Información general.

CATEGORÍA	INSTITUCIÓN	RESPUESTA	
		CARGO	FUNCIONES

Información General	Policía Nacional Civil, Departamento de Investigaciones, Delegación San Miguel	Jefe de Investigación en funciones de Delitos generales.[13]	Mi labor es jefatura; yo superviso los casos. Algunas veces me involucro en los casos, a veces voy al terreno con ellos a apoyarles, y el mayor tiempo estoy aquí en el escritorio, coordinando y dirigiendo.
		Grado académico	Sub inspector de la Policía Nacional Civil de El Salvador y actualmente, estudiante de la carrera
		Lugar dónde se encuentra destacado	Departamento de Investigaciones de la Delegación de San Miguel

ii. Entrevista.

CATEGORÍA	INSTITUCIÓN	PREGUNTA	RESPUESTA
Entrevista presencial	Policía Nacional Civil, Departamento de Investigaciones, Delegación San Miguel	1. Cantidad de personas que conforman el equipo de investigación delito de revelación indebida de datos o información de	Tres personas conforman el equipo de investigación de delitos. Esas tres personas están para todos los delitos; trabajan inclusive los de la Les especial de Delitos Informáticos y Conexos. Por ejemplo, si alguien y mire fíjese que han publicado una foto mía desnuda en facebook, digamos, ya

[13] Se omite escribir el nombre del funcionario, respetando los términos en que se otorgó la entrevista.

		carácter personal, y ¿cuáles son sus funciones?	al investigador se le asigna el caso y ya empieza a trabajar, toma la entrevista, a obtener otro tipo de información, rastrear Facebook u otras redes sociales, depende del lugar de dónde haya sido. Lo que quiero que quede claro, es que solo ellos tres, son para todos los delitos. Claro que hay delitos que no se dan, hay unos que se dan más que otros, hay delitos que son bien comunes, por ejemplo, hoy, hasta las expresiones de violencia contra la mujer, hasta ese tipo de delitos también se investigan.
		2. ¿Qué tipo de formación reciben para realizar la investigación del Delito de Revelación Indebida de Datos o Información de Carácter Personal, por este delito el más cometido?	Fíjese que hay una División de Central de Investigaciones que se llama DCI; allá en la DCI, está podría decirse, las personas que capacitan al personal para diferentes fines; a ellos se les hace una solicitud que necesitamos una capacitación para "X" delito, porque no todos los delitos son iguales, cambian, son variantes. Entonces ellos comienzan a darnos la capacitación; claro, ellos han sido instruidos y capacitados fuera del

		país, en la Interpol, también con otras entidades como en Estados Unidos y otros países. Nosotros, en San Miguel, hasta el momento, nadie ha salido fuera del país a capacitarse, pero internamente acá en el país, las capacitaciones que hemos recibido son de parte de la División Central de Investigaciones; se puede decir, que ellos son expertos en la materia. Ellos tienen todas las herramientas También han venido capacitadores de fuera de país. Las capacitaciones que recibimos, para mi, para mi, la verdad, la verdad, no son tan adecuadas porque debería ser una persona idónea específicamente que ya tenga varios años de trabajar en este tipo de delitos, porque hay personas que nunca han trabajado este tipo de delitos, razón por la cual les cuesta cuando se enfrentan a este tipo de delitos. En cambio, las personas que tienen más experiencia en la rama, pues ya ellos pueden desenvolverse mejor,

		brindar una mejor opinión en alguna duda que uno tenga, o algo que se pueda hacer, mediante internet o si violenta alguna ley internacional o nacional.
	3. ¿Cuáles son las herramientas jurídicas, técnicas y científicas utilizadas para la investigación del Delito de Revelación Indebida de Datos o Información de Carácter Personal?	Hay un software especial, que se utiliza para esto, claro tiene que ser mediante una dirección funcional de la Fiscalía, no es así no más que usted va a introducirse a la información de la persona y extraerla; no, tiene que venir mediante la Fiscalía, porque si no, ya está robando información, y eso sí es delito. Siguiendo la orden de la Fiscalía, allí si es una prueba, porque si no, si lo detecta un abogado, puede caerse el caso. La situación es esta: la Fiscalía le solicita al Juez, luego el Juez le da el aval, para poderlo hacer. Eso es igual, por ejemplo, si alguien anda delinquiendo, digamos un pandillero anda un número de teléfono, entonces la Fiscalía lo que hace es solicitarse al Juez, que va a utilizar la herramienta, para poder hacer las escuchas de ese número, para

		la sustracción; porque de otra forma, es ilegal. El software existe, pero nunca se ha profundizado debidamente, porque depende mucho de la Fiscalía, porque de la dirección funcional que ellos nos dan, nosotros podemos trabajar la investigación; de lo contrario, si ellos no nos la dan, o nos limitan cierta información, ya que no es lo mismo, que digan "y otras diligencias" necesarias que puedan realizar, entonces sí, allí hay libertad, de lo contrario, no. Es que … la situación es ésta: este tipo de delitos, no es muy común, hay mucha gente, hay mucha población, que desconoce hasta que existe esta Ley, inclusive, fiscales, jueces, abogados, que nunca han trabajado en hechos de éstos, o sea, la desconocen totalmente. Por esa razón, no es tan común que se diga las personas con el hecho de desconocer que en realidad lo que les ha sucedido, en su Facebook, en su WhatsApp, en Messenger, en otras redes sociales, se puede tipificar como delito, y

		muchas personas lo ignoran y es por eso que no lo denuncian y lo ven como algo común y hasta risa les da y se ponen a reír con caritas alegres de lo que la otra persona está diciendo de la otra persona o de la población. También si no hay una denuncia, por el mismo motivo, que las personas desconocen, falta divulgar la Ley Especial Contra los Delitos Informáticos y Conexos: eso es lo importante, y es lo que no se hace. Inclusive, mucha gente ni se imagina que existe esta Ley. A raíz de esa ignorancia de la población, no denuncian, no saben que lo legal es que están ante un delito grave y que no saben que les están violentando sus derechos de intimidad personal, de información y datos de carácter personal en cualquier tipo de sus redes sociales.
	4. ¿Por qué el delito de Revelación Indebida de Datos o Infor-	Es que el Delito de Revelación Indebida de Datos o Información de Carácter Personal, es el más cometido a través de las redes

		mación de Carácter Personal es el más cometido?	sociales, porque en las redes sociales hay mucha comunicación de todo el mundo. A raíz de eso, este Delito de Revelación Indebida, inclusive, personas que disfrazan la información, la suplantan y la utilizan como que si fueran otras personas. Como ahora esta situación es una comunicación social a nivel mundial; la mayoría de personas, si usted se fija, ni llamadas hacen, ya que se comunican más a nivel de redes sociales como WhatsApp, Messenger, Facebook, Instagram, hacen video llamadas, y ya toda esa información, la persona la transmite por estos diferentes medios. Claro, aunque siempre hay algunas personas que tienen privada su información. Otras, como desconocen el uso y las condiciones de privacidad de la información, lo dejan en libertad. Entonces ¿qué hacen algunas personas? Utilizar información, vaciarla, inclusive los hackers la toman para poderla utilizar hasta posiblemente para una guerra. Este delito de Revelación Indebida

		de Datos o Información de Carácter Personal, es el más delicado y el más común. Es el que más se da. Incluso, hay personas que se dedican a comprar información, fotografías…, vía internet, pagan por ese tipo de información; es más, esa información es bien pagada. Aquí en San Miguel, y a nivel nacional, el delito Revelación Indebida de Datos o Información de Carácter Personal, es el más denunciado y el más cometido y no sé si a nivel mundial, allí, habría que investigar.
	5. ¿Cuál es el procedimiento, trato o enfoque que se le da al delito de Revelación Indebida de Datos o Información de Carácter Personal?	Inicia con la denuncia de la persona, ya sea en la Fiscalía General de la República, Policía Nacional Civil o un Juzgado de Paz; es decir, en cualquiera de esas tres instancias. El ciudadano tiene tres opciones, puede denunciar al Juzgado de Paz de donde vive la víctima, o bien podía avocarse a la Fiscalía o bien a la Policía. Todos están obligados a recibir la denuncia. Cabe aclarar que cada entidad

		tiene un procedimiento diferente, pero siempre se apoyan en la Policía, porque es la que se dedica a investigar los hechos, por medio de la función direccional del fiscal. Es decir, que el fiscal maneja la Ley Especial de Delitos Informáticos y Conexos. Guía la información, no es que él sea el investigador. Luego, digamos que viene a la Policía. Primero, se recibe la denuncia y después se le asigna un investigador. Como son tres los investigadores, digamos hoy le toca a investigador "A", luego al "B", y así sucesivamente; es decir, que va una rueda de casos a cada uno; es decir, van alternados. En esta situación, el investigador asignado, llama a la víctima, es decir, a la persona ofendida, y en el momento, le toma una entrevista para relacionar los hechos que se quiere que se investiguen y que se siente ofendida por eso. Se procede a la investigación según lo que vaya requiriendo el fiscal. Cuando ingresa la denuncia,

			tenemos ocho horas para enviar la información al fiscal, porque la Policía tiene la obligación de informar de ese delito, para que inmediatamente se le asigne un fiscal, ya asignado el investigador que va desde el momento de la denuncia, para que se inicie ya una investigación. ,
		6. ¿Cuáles son las limitaciones que se tienen en la investigación del delito de Revelación In-debida de Datos o Información de Carácter Personal?	No existe un personal idóneo que esté capacitado sobre los delitos que contiene la Ley Especial contra delitos Informáticos y Conexos, porque esta Ley es nueva, no tiene ni cinco años, ¿usted cree que hay personal capacitado idóneamente para trabajar estos delitos? Porque aquí lo que toca es ir aprendiendo en el camino. Porque sí, existe una unidad especializada, que sí trabaja estos delitos. Esa unidad sí es especializada para trabajar todo tipo de delitos informáticos, por ejemplo, cuentas bancarias, cuentas de Facebook, WhatsApp, estafas, extorsiones, todo lo relacionado…todo. Aquí tenemos limitaciones como

		falta de personal, falta de medios idóneos para desempeñar mejor la función investigativa, porque allá en San Salvador, es un equipo compacto, están llevan los casos más delicados; ellos sí tienen todas las herramientas, los medios como software, aplicaciones, equipos móviles que nosotros no tenemos acá en San Miguel. Tienen una infinidad de medios con los que cuentan para poder investigar y hacer más fácil el trabajo, en cuanto a la cuestión informática. Nosotros, acá en San Miguel, no tenemos esos medios, razón por la cual nos auxiliamos de ellos; por ejemplo, yo pedí autorización a la DCI, para poder brindarle y apoyarle con la información a usted. Es por eso que yo no quería brindar información. Inclusive se me dijo que no detallara casos; “dele información a grosso modo, no específicamente qué se hace” Es que vaya, la Dirección Central de Investigaciones, donde está la subdirección de Investigaciones, podríamos decir que es el cerebro,

		nosotros somos una rama. Todos los departamentos de investigaciones a nivel nacional, dependemos de la SIN. Nos auxiliamos de ellos y todo lo que hacemos, como capturas, detenciones, ellos lo saben. Todos los casos que tenemos, ellos lo conocen, toda la información que tenemos, ellos la ven, todo, todo, todo. De allí nos supervisan cómo va cada caso: “quiero saber que se ha hecho en este caso” y si está mal y no se puede desarrollar, o no puede investigar, ellos mandan un equipo de apoyo, para apoyar en el quehacer de la investigación. Inclusive, pueden pedir diligencias de un caso y nos dicen que no lo podemos llevar nosotros en investigación, sino que ellos. Tanto así que la Unidad Especializada, existe antes que esta Ley. Habrá unas 20 o 25 personas que conforman esa unidad. Inclusive todos los casos importantes a nivel nacional, allí llegan, porque si vienen a aquí, el

		Director los margina y le pone “investíguese, DCI, delitos informáticos” Acá podemos decir que se investigan casitos que son bagatelas. Nosotros acá en San Miguel, estamos en pañales; es decir, estamos comenzando a conocer de esta Ley Especial de Delitos Informáticos.
	7. ¿Cuál es el procedimiento, seguimiento y finalización que le dan a las denuncias que ingresan por el delito de Revelación Indebida de Datos o Información de Carácter Personal?	Cuando entra aquí, se toma la denuncia; se le asigna el investigador, quien cita a la víctima para una entrevista, se le da ubicación, seguimiento y vigilancia para poder llegar a un término que es identificar al culpable y allí es que se vuelve activo. el caso puede estar en investigación pero a medida que transcurre el tiempo, se vuelve pasivo, porque no se le trabaja, porque ya se efectuó la entrevistas se le dio ubicación, seguimiento y vigilancia Pero en muchos casos, quedan en estado pasivo mientras

			no surja algún nuevo hecho. O que de la División Central de Investigaciones (DCI) soliciten el expediente o información de las diligencias que hemos realizado. De no ser así, se archiva.
		8. ¿Cree que actualmente existe impunidad en el cometimiento del delito de Revelación Indebida de Datos o Información de Carácter Personal?	Hay una total impunidad, la impunidad es terrible, como le decía anteriormente, porque la Ley es nueva, por falta de divulgación de la Ley; y, por tanto, falta conocimiento de la misma. Las personas lo dejan en impunidad, porque, la verdad, desconocen la Ley totalmente. Porque puede convertirse en delito, ya sea mediante un móvil, una computadora, sistemas informáticos, porque aquí los salvadoreños, hasta que no tenemos la experiencia, no podemos decir “ay, ya me pasó esto”. Esa es como una parte social; pero ya internamente, es porque la situación se debe a muchos factores, no sé cómo explicarle…, pero la impunidad sí existe, no solo en este delito, sino en todos los de la Ley.

iii. Hallazgos

En la PNC Delegación San Miguel, no existe un equipo especializado de personas para investigar los delitos informáticos en el contexto general de la Ley Especial; y, en consecuencia, para efectos de esta investigación, tampoco existe equipo especializado para la investigación del Delito de Revelación Indebida de Datos o Información de Carácter Personal.

Únicamente existen tres personas que conforman el equipo de investigación de delitos, quienes están para atender todo tipo de delitos que la población llega a denunciar a la sede policial.

En cuanto a las capacitaciones al personal en la temática de Delitos Informáticos, se encontró que: a) No existe una formación sistemática de la LEDIC. b) El centro de formación de Delitos Informáticos, está concentrado en San Salvador y se encuentra dentro de la División Central de Investigaciones “DCI”; c) De tener la necesidad de capacitaciones, se solicita directamente a la DCI; e) El equipo de investigadores de delitos de la sede policial San Miguel, nunca ha recibido de primera mano una capacitación fuera del país.

La herramienta que maneja el Departamento de Investigaciones se apega más que todo a los procedimientos preestablecidos entre la PNC y la FGR. En cuanto a las herramientas tecnológicas/científica, no trabajan con ellas, se tiene el conocimiento que existen softwares especiales para las investigaciones de Delitos informáticos, en general.

De acuerdo a la Departamento de Investigaciones, el Delito de Revelación Indebida de Datos o Información de carácter Personal, es el más cometido debido al auge de las comunicaciones a nivel mundial y a la diversidad y a la vasta cantidad de redes sociales.

El trato que se le da al delito objeto de este estudio, es uno más. No tiene un enfoque, un trato especializado o trato diferenciado; sino que se sigue el mismo procedimiento que se le da a cualquier otro. No existe una relevancia o técnica específica para esta investigación.

Se encontró una diversidad de limitaciones en la investigación del Delito de Revelación Indebida de Datos o Información de Carácter Personal entre los que se pueden enumera: a) No existe un personal idóneo, capacitado en la LEDIC. b) Es una ley relativamente nueva y en el tiempo que lleva en vigencia, no ha alcanzado la madurez. c) No se cuenta con los medios básicos, ni tampoco con herramientas técnica/científicas que permita una investigación idónea acorde a las exigencias tecnológicas que requiere esta Ley Especial. d) Los recursos humanos y herramientas científicas tecnológicas, están centralización en San Salvador en la División Central de Investigaciones.

El procedimiento, seguimiento y finalización de la denuncia del delito que ingresa, se encontró que no existe ninguna particularidad respecto a los delitos comunes, es decir, el seguimiento y finalización, es el mismo para todos.

Se acepta de forma clara la existencia de total impunidad, básicamente porque la Ley es nueva, no hay divulgación de la misma y la población la desconoce.

b) Unidad Especializada de Delitos Informáticos Policía Nacional Civil

i. Información general

CATEGORÍA	INSTITUCIÓN	RESPUESTA	
		CARGO	FUNCIONES
Información General	Policía Nacional Civil Unidad de Acceso a la Información Pública	Jefe de la Unidad especializada de Delitos Informáticos, San Salvador, Inspector Laínez, quien dio respuesta a través	Dirige la Unidad Especializada de Delitos Informáticos.

		de la Unidad de Acceso a la Información Pública de la Policía Nacional Civil, mediante la autorización del Jefe de la División Central de Investigaciones San Salvador, Señor Comisionado Douglas Elenilson Zometa	

ii. Entrevista

CATEGORÍA	INSTITUCIÓN	PREGUNTA	RESPUESTA
Entrevista digital mediante cuestionario	Policía Nacional Civil Unidad de Acceso a la Información Pública	1. Número de agentes que trabajan en la investigación del Delito de Revelación In-debida Datos o Información de Carácter Perso-nal y ¿cuál es la función que desempeñan?	Está conformado por ciento diecisiete (117) investigadores, conformados por Equipos de Investigación que se abrevia EVIM y la Unidad de Delitos Informáticos de esta División.
		2. ¿Qué tipo de	Se da respuesta en base al Oficio

		formación reciben para realizar la investigación del Delito de Revelación Indebida de Datos o Información de Carácter Personal, por este delito el más cometido?	No. 0446 literalmente dice " La Formación técnica y científica es por la Academia Nacional de Seguridad Publica que se abrevia ANSP y otras Instituciones Nacional e Internacionales, son relacionados a capacitar en los Cursos para la investigación de Delitos Informáticos y las Tecnologías de la Información y comunicación que se abrevia TIC 'S".
		3. ¿Cuáles son las herramientas jurídicas, técnicas y científicas utilizadas para la investigación del Delito de Revelación Indebida de Datos o Información de Carácter Personal?	Se da respuesta en base al Oficio No. 0446 literalmente dice"" *Tratándose que el delito es de conocimiento oficioso con base a lo que establece Ley Especial Integral Para una Vida libre de Violencia que se abreva LEIV y la Ley Especial de Delitos Informáticos y conexos, la investigación se inicia a través de la denuncia.*"""""
		4. ¿Por qué el delito de Revelación Indebida de	Se da respuesta en base al Oficio No. 0446 literalmente dice "Con base a los registros estadísticos que se tiene en

		Datos o Información de Carácter Personal es el más cometido?	nuestras bases de datos y que le anexo en un folio no es preciso manifestar que el delito de Difusión ilegal de Información, sea el más cometido."
		5. ¿Cuál es el procedimiento, trato o enfoque que se le da al delito de Revelación Indebida de Datos o Información de Carácter Personal?	Se da respuesta en base al Oficio No. 0446 literalmente dice *"El procedimiento es obedeciendo a la Dirección Funcional girada por la Fiscalía General de la Republica, y el trato en la investigación técnica es haciendo uso de las TIC 'S. y la finalidad es la erradicación del delito en referencia".*
		6. ¿Cuáles son las limitaciones que se tienen en la investigación del delito de Revelación Indebida de Datos o Información de Carácter Personal?	Se da respuesta en base al Oficio No. 0446 literalmente dice "La limitación que se tiene que el país no es parte del Convenio de BUDAPEST, razón por la cual existen limitaciones a nivel de Cooperación Internacional".
		7. ¿Cuál es el procedimiento, se-	Se da respuesta en base al Oficio No. 0446 literalmente dice

		guimiento y finalización que le dan a las denuncias que ingresan por el delito de Revelación Indebida de Datos o Información de Carácter Personal?	"Recibimiento de la Denuncia, notificación a la Fiscalía General de la Republica, investigar el caso haciendo uso de las herramientas tecnológicas TIC 'S operativizar el caso y su finalización."
		8. ¿Cree que actualmente existe impunidad en el cometimiento del delito de Revelación Indebida de Datos o Información de Carácter Personal?	Se da respuesta en base al Oficio No. 0446 literalmente dice *"A la fecha se tienen datos estadísticos que arrojan que se han operativizados casos y otros que están en proceso de investigación, por lo tanto no pertinente expresar que como Institución policial, se expresa que exista en la actualidad impunidad, razón por la cual en el cuadro anexo se registra el 21.57 de efectividad"*

iii. Hallazgos.

Las respuestas obtenidas a través de la Unidad de Acceso a la Información Pública, de la Policía Nacional Civil, son escuetas; se limitan a lo que está descrito en la

Ley, son respuestas meramente documentales; y, por tanto, no permiten conocer a fondo el quehacer de la institución.

Efectivamente existe una unidad especializada de delitos informáticos acorde a la LEDIC, y que cuenta con 117 investigadores, en la sede central de la Policía Nacional Civil de la ciudad de San Salvador; sin embargo, la situación cambia en la sede de San Miguel, donde no existe unidad especializada. Se encontró a través de la entrevista que en la sede central, sí se tienen las competencias pertinentes y un régimen de capacitaciones constantes; además, cuentan con las herramientas tecnológicas y científicas idóneas, como, móviles, equipos y software especializados, únicamente para la investigación de estos delitos, los cuales no fueron incorporadas en este trabajo, porque cuentan con una reserva de información.

La denegación de la información, fue fundamentada por el oficial de información, Comisionado Luis Ernesto Núñez Cárcamo (Ver anexo 1. Policía Nacional Civil. Resolución Final Ref. C-210-2019, página 2 de la resolución) basándose en el memorándum SIN/DCI/0232/2020 de fecha 16 de abril, suscrito por el Jefe de la División Central de Investigaciones, Comisionado Douglas Elenilson Zometa, (Ver anexo 2 Policia Nacional Civil. Memorandum. SIN/DCI/0232/2020 en las páginas de la segunda a la sexta de dicho documento)

De acuerdo a la División Central de Investigaciones, la limitación parte del hecho que El Salvador no forma parte del Convenio de Budapest y por lo tanto, existen limitaciones a nivel de cooperación internacional.

c) Fiscalía General de la República, sede San Miguel

i. Información general.

CATEGORÍA	INSTITUCIÓN	RESPUESTA	
		CARGO	FUNCIONES
Información General	Fiscalía General de la República, Sede San Miguel.	Jefe de la Oficina Fiscal de San Miguel.	Responsable de realizar la gestión operativa fiscal dando cumplimiento a responsabilidades y funciones administrativas dentro de la comprensión territorial de la oficina fiscal de San Miguel, coordinar la investigación de hechos punibles en colaboración con la PNC, así como ejercer las acciones legales con el objeto de defender los intereses dela sociedad, en coordinación con los Directores, Jefes de Oficinas Fiscales de otros departamentos, Jefes de Unidades, Coordinadores y Fiscales Auxiliares

ii. Entrevista

CATEGORÍA	INSTITUCIÓN	PREGUNTA	RESPUESTA
Entrevista	Fiscalía General de la República, Sede San Miguel	1. Cantidad de personas que conforman el equipo de investigación delito de revelación indebida de datos o información de carácter personal, y ¿cuáles son sus funciones?	No hay equipo de investigación o Unidad Especializada en la oficina Fiscal de San Miguel para conocer de los delitos informáticos en general, ni tampoco para el delito en específico de su interés, siendo la Revelación Indebida de Datos o Información de Carácter Personal, regulado en el Art. 26 de la Ley Especial Contra los Delitos informáticos y Conexos; no obstante, de ello tienen competencia, de manera general, para conocer internamente de dicho Delito, los fiscales auxiliares de la Unidad de Vida e Integridad Física, así como otras Unidades, por ejemplo, si existen relaciones familiares entre el sujeto activo y la víctima, conocería la Unidad de Delitos Relativos a la Niñez y Adolescencia y Mujer en su Relación Familiar, etc.
		2. ¿Cuáles son las herramientas jurídicas, técnicas y científicas utilizadas para la	Dentro de las ***herramientas jurídicas***, de primera mano, la Ley Especial Contra los Delitos Informáticos y Conexos, y las diversas facultades que otorga en la investigación con el uso de las tecnologías de la

		investigación del Delito de Revelación Indebida de Datos o Información de Carácter Personal?	información y comunicación para la recopilación de evidencias, así como el catálogo de facultades que otorga el Código Procesal Penal en materia de investigación, en colaboración con la Policía; recordemos que el fiscal auxiliar es el que dirige la investigación con la emisión de direcciones funcionales que son opiniones técnico jurídicos; también, no podemos olvidar, el principio de libertad probatoria que rige el proceso penal, siempre y cuando se cumpla con la obtención de los elementos probatorios de legal forma, respetando los derechos fundamentales de la víctima y persona a investigar, el catálogo de herramientas jurídicas, puede ser amplio. En cuanto a las ***herramientas técnicas y científicas.*** la Fiscalía para la recolección de evidencias o elementos probatorios dentro de una investigación, puede auxiliarse de la Sección de Análisis y Tratamiento de la Información (SATI) de la Policía Nacional Civil de San Miguel o en su caso de Dirección de Análisis, Técnicas de Investigación e

		Información (DATI) que es una institución adscrita a la Fiscalía que apoya en la gestión para obtener respuesta en todo lo relacionado a aspectos de Tecnologías de la Información y la Comunicación; auxilian, por ejemplo, desde la obtención de la IP, tipo de teléfono de conexión, lugar de activación de dónde se utilizó una cuenta, por ejemplo. De Facebook, como red social, teniendo los enlaces respectivos, para lograr identificar a sujeto activo que ha revelado datos o información de carácter personal.

		3. ¿Qué tipo de formación reciben para realizar la investigación del Delito de Revelación Indebida de Datos o Información de Carácter Personal, por este delito el más cometido?	Estamos en proceso constante de capacitación de los fiscales auxiliares o personal técnico jurídico, en razón que la Ley Especial Contra los Delitos Informáticos y Conexos, regula tipos penales modernos que pretenden proteger la confidencialidad, integridad, seguridad y disponibilidad de los datos informáticos de las personas o empresas, en razón que los instrumentos electrónicos han adquirido relevancia, para el desarrollo económico, social del país, impuestos por la globalización; por lo que la formación fiscal no debe ser estática por lo que dichas capacitaciones se realizan por medio de la ***Escuela de Capacitación Fiscal***, que es la encargada de convocar al personal fiscal o técnico jurídico para la formación en temas relacionados con los delitos informáticos.

	4. ¿Por qué el delito de Revelación Indebida de Datos o Información de Carácter Personal es el más cometido?	Se debe al uso masivo de dispositivos electrónicos usados por la población, como teléfonos, Tablet, laptop,etc, que reciben y envían información personal y almacenan datos privados como imágenes, audios, videos; en la mayoría de casos, dichos dispositivos se conectan a la red de internet o redes sociales, y allí es que personas mal intencionadas ingresan o acceden por cualquier medio de forma indebida o fraudulenta, obteniendo información privada y exponen esos datos, inclusive de naturaleza sexual de la víctima, incurriendo en el delito objeto de investigación, agravando el tipo penal; incluidos también la grabación por obtener y revelar datos confidenciales, personales de la Unidad de Acceso a la Información Pública.
	5. ¿Cuál es el pro-	Siempre tratando de proteger los

		cedimiento, trato o enfoque que se le da al delito de Reve- lación Indebida de Datos o Información de Carácter Personal?	derechos fundamentales de las víctimas como la intimidad, honor, integridad sexual, propiedad intelectual, seguridad pública,; asimismo, tratando de utilizar herramientas de investigación modernas que ayuden a lograr individualizar al sujeto responsable de la exposición de datos personales privados, así como los daños morales o sociales que hayan ocasionado a la víctima.
		6. ¿Cuáles son las limitaciones que se tienen en la investigación del delito de Revelación Indebida de Datos o Información de Carácter Personal?	Es difícil controlar qué puede existir sobre la red de internet, en razón que una vez la imagen o video personal confidencial ha sido expuesto; el eliminarlo de la red del internet es complejo y difícil, puesto que no se tienen protocolos que regulen la eliminación de servidores privados que tienen su dominio y domicilio fuera del país, manejados por empresas transnacionales; por lo que encontrar al responsable inicial de extraer los datos o información personal, resulta una tarea compleja con el uso de herramientas tecnológicas, pues se deben ubicar direcciones de IP, puntos de conexión, dispositivos

			electrónicos desde dónde se conectan, a nombre de quien posiblemente está registrado, lo que dificulta en algunas ocasiones individualizar al sujeto responsable directo.
		7. ¿Cuál es el procedimiento, seguimiento y finalización que le dan a las denuncias que ingresan por el delito de Revelación Indebida de Datos o Información de Carácter Personal?	El procedimiento inicial, es tratar de individualizar al posible responsable, a través de los direccionamientos funcionales dirigidos a la Policía Nacional Civil, coordinaciones con el SATI o DATI, entrevistas de testigos, recolección de evidencias o elementos probatorios, para efectos de recopilar toda la información y valorar ejercer la acción penal ante los tribunales competentes; pero en muchas ocasiones, el resultado de los casos aperturados es insatisfactorio para las víctimas, puesto que en el plazo legal para investigar, que son cuatro meses, no se logra individualizar al responsable directo que ha extraido la información, porque utilizan en muchas ocasiones, cuentas falsas, direcciones de IP modificadas o de otros países, donde publican los datos indebidos o personales, por lo

			que el fiscal auxiliar procede a archivar el caso administrativamente de conformidad al Art. 293 numeral 1 del Código Procesal Penal, a la espera de otro nuevo elemento que haga variar la investigación.
		8. ¿Cree que actualmente existe impunidad en el cometimiento el delito de Revelación Indebida de Datos o Información de Carácter Personal?	Se debe trabajar arduamente en el aspecto investigativo técnico científico para esclarecimiento del Delito de Revelación Indebida de Datos o Información de Carácter Personal, así como la creación de protocolos de entendimiento directos con las empresas transnacionales que manejan los dominios o redes sociales fuera del país o limiten el uso de datos en la red de internet, para que la información requerida sea precisa y fácil para dar con la individualización del sujeto activo del delito, así lograr evitar la impunidad en este tipo de hecho y dar un respuesta a la víctima para lograr justicia que busca al acudir ante la fiscalía

iii. Hallazgos

Es importante mencionar que el jefe de la Unidad Fiscal, debido a la carga laboral y emergencia nacional, expresó que la única forma en que podía apoyar, en el presente trabajo, como institución, era que se le hiciese llegar el cuestionario de la entrevista, asimismo no era prudente, por la misma emergencia, entrevistar otros fiscales, ya que además no existía un equipo específico para tratar los delitos informáticos, y que las respuestas serían similares, por lo cual, él respondería posteriormente entregando los resultados mediante documento físico, por escrito.

Como se expresó en párrafo anterior, no existe ninguna unidad especializada que se dedique a la investigación de Delitos informáticos y en consecuencia, no existe un equipo de fiscales auxiliares para investigar el Delito de Revelación Indebida de Datos o Información de Carácter Personal. Cada unidad designa fiscales para atender determinados delitos.

La herramienta jurídica es precisamente la Ley Especial Contra Delitos Informáticos y Conexos. Apegándose a los procedimientos que establece el Código Procesal Penal para dirigir la investigación, auxiliándose de la Sección de Análisis y Tratamiento de Información (SATI) y la Dirección de Análisis Técnicas de Investigación e Información (DATI) que es una institución adscrita a la Fiscalía.

Si bien es cierto que se reciben capacitaciones de parte de Escuela de Capacitación Fiscal, esta formación es para todo tipo de delitos, pero no de una forma relevante para la Ley Especial Contra los Delitos Informáticos y Conexos, y menos entonces para el Delito de Revelación Indebida de Datos o Información de Carácter Personal; es decir, se reciben todo tipo de capacitaciones incluyendo la de los delitos informáticos en general.

De acuerdo a la fiscalía, el delito en cuestión es el más cometido debido al exacerbado uso de dispositivos electrónicos y la facilidad de acceso a las redes sociales del que hace uso masivo la población; producto de esta situación es que se genera el cometimiento de este delito, pero también se hace alusión que se trata de proteger los derechos de las víctimas expuestas al cometimiento de este delito.

Se contrasta el hecho de adoptar la postura de salvaguardar los derechos de las víctimas en este delito, con el hecho que, en la realidad, existe una gran pasividad respecto a la investigación del cometimiento de estos hechos.

Se acepta de parte de la institución en referencia, que es muy difícil controlar lo que puede existir en la internet, puesto que no existe un protocolo que regule la limitación de servidores privados y que además tienen su dominio y domicilio fuera del país, y además son manejados por empresas transnacionales. Por lo que controlar al responsable, resulta una tarea compleja con el uso de herramientas tecnológicas.

Pese a los esfuerzos establecidos como los procedimientos iniciales, individualización de los posibles responsables mediante los direccionamientos funcionales dirigidos a la policía nacional y coordinaciones con el SATI o DATI, así como entrevistas a testigos, recolección de evidencia o elementos probatorios, entre otros, cabe mencionar que no prosperan, ya que agotando todo el procedimiento, lo que se hace al final, es archivar los casos, basados en el artículo 293 numeral 1 del Código Procesal Penal.

Queda al desnudo, que se reconoce que sí existe una *impunidad en la investigación* en el Delito de Revelación Indebida o Información de Carácter Personal, debido a que se asume que no existe un esclarecimiento en la investigación de este tipo de delitos, debido a que no hay protocolos de entendimiento directo con las empresas transnacionales que manejan los dominios o redes sociales fuera del país o limiten el uso de datos en la red del internet, para que la información requerida sea precisa para dar con la individualización del sujeto activo del delito. En términos generales, se acepta que existe impunidad.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Mediante la investigación de campo del presente trabajo que identificó que tanto en la Policía Nacional Civil como en la Fiscalía General de la República con

sede en la ciudad de San Miguel, existen límites para la investigación del Delito de Revelación Indebida de Datos o Información de Carácter Personal.

Entre estos límites se identificaron interesantes elementos, como son:

a) El hecho que, por ser una Ley reciente que data del año 2016, aún no ha sido desarrollada a nivel procedimental y procesal. Se legisló por la necesidad que había de darle respuesta a los hechos punibles cometidos a través del uso de las herramientas tecnológicas; sin embargo, aún no se ha logrado obtener los resultados esperados. En otras palabras, se ejecutó sin estar institucional y técnicamente preparados a nivel nacional, ya que el cometimiento de los delitos informáticos se da en todo el país y no solo en la capital de la República, donde se han enfocado los esfuerzos en la investigación y seguimiento de ese tipo de delitos. Esto se puede constatar con los datos estadísticos recaudados, al comprobarse que en la ciudad de San Miguel, no existen requerimientos, ni judicializaciones, ni condenas, ni absoluciones en el Delito de Revelación Indebida de Datos o Información de Carácter Personal, que es objeto de estudio de esta investigación.

b) De acuerdo al objetivo general, enfocado en la ciudad de San Miguel, las limitaciones son más evidentes, puesto que no existe una unidad especializada ni en la Fiscalía ni en la Policía y, por tanto, tampoco existe un equipo de investigadores para los delitos informáticos, y en consecuencia, tampoco existe para el delito de Revelación Indebida de Datos o Información de Carácter Personal. En cuanto al conocimiento que poseen, de parte de los investigadores y fiscales, tienen claro el conocimiento de la ley, el desarrollo doctrinario del tipo penal en cuestión; sin embargo, se presentan problemas técnico operativos para lograr la individualización de los autores o partícipes en estos hechos, el uso de las tecnologías para efectos de investigación es deficiente; primero, porque no existe un límite en el uso del internet, y segundo, porque las empresas que controlan dicho uso están fuera del país, y son quienes controlan el auge de los medios informáticos y comunicación.

c) El delito más cometido y más denunciado por la población de San Miguel, ha sido el de Revelación Indebida de Datos o Información de Carácter Personal, en el período de enero de 2018 a febrero de 2020, según lo reflejado en los datos estadísticos proporcionados por la Unidad de Acceso a la Información Pública de la FGR a través del Departamento de Estadística, de acuerdo a los registros de las bases de datos del Sistema de Información y Gestión Automatizada del Proceso Fiscal (SIGAP) información emitida al 25/06/2020 (ver anexo 5), pues del total de delitos informáticos denunciados (147), el 37.41% (55), corresponden al delito objeto de esta investigación; es decir, de 147 denuncias, 55 corresponden al Delito de Revelación Indebida de Datos o Información de Carácter Personal.

d) En cuanto a los casos en investigación activa, como refiere el cuadro del anexo 6 para el mismo período (enero de 2018 a febrero de 2020), el delito en estudio presenta la mayor cantidad de casos activos, ya que, de 81 casos de todos los delitos reportados, 36 (44.44%) corresponden al Delito de Revelación Indebida de Datos o Información de Carácter Personal (ver anexo 6). No obstante, se encontró en las estadísticas del SIGAP que, en cuanto a requerimientos presentados, condenas, absoluciones, del delito en estudio, no se hallaron registros en el mismo período (ver anexo 8, página 5 numeral 1) encontrando que únicamente se han presentado dos dictámenes de acusación, pero de esos dos, ninguno corresponde al delito objeto de este trabajo (ver anexo 7) enmarcados en el período de inicio y fin de este proyecto de investigación (enero 2018 a febrero 2020).

e) En relación a la información vertida por Unidad de Acceso a la Información Pública - OIR PNC, de acuerdo a sus estadísticas (Anexo 3) en el período del 1 de enero al 31 de diciembre de 2019, se comprueba que los delitos informáticos están categorizados dentro de los delitos en general, y que el delito centro de esta investigación, tiene un conteo considerable (23) sólo superado por los delitos de amenaza (36) y el de estafa (26), por lo cual es evidente que el cometimiento del delito informático en referencia, en la

ciudad de San Miguel, tiene una alta frecuencia, aun comparándolo con los delitos comunes.

f) El anexo 4, de delitos informáticos, emitido por la UAIP-OIR-PNC, muestra las estadísticas del período 2019-2020, en los que siempre resalta la mayor incidencia en denuncia con un total de 29 y 11 respectivamente, del Delito de Revelación Indebida de Datos o Información de Carácter Personal, en las cuales la PNC reporta los casos iniciados, denunciados, investigados, en investigación y a disposición de la Fiscalía. Para el año 2019 únicamente fueron investigados 3 casos de los 29, lo que equivale al 10.34%; el resto, 26 que corresponde al 89.66% quedaron en investigación, y el total, (29) fueron puestos a disposición de la Fiscalía. La tendencia continuó en los primeros meses del año 2020, ya que al mes de julio la información proporcionada, fue de 11 casos denunciados y ninguno (0%) había sido investigado. Ahora bien, en el consolidado de ambos años se tiene un 7.5% (3) casos investigados de un total de 40. Y no se encuentran más registros que indiquen más investigaciones en el delito, fijado en el período de enero 2018 a febrero 2020, en el presente estudio.

En cuanto al tratamiento que se le da al Delito de Revelación Indebida de Datos o Información de Carácter Personal, en la ciudad de San Miguel, en la Policia Nacional Civil, mediante la investigación en campo, se logró identificar que el trato y enfoque del proceso de inicio e investigación del delito en referencia, no es distinto del trato que se les da a otros delitos que no están contemplados en la Ley Especial Contra los Delitos Informáticos y Conexos.

Asimismo, mediante la investigación, se identificó que el recurso humano con que cuenta la institución relacionada (PNC), está constituido por tres personas que forman el equipo de investigación para todos los delitos, incluyendo el de Revelación Indebida de Datos o Información de Carácter Personal.

Por otra parte, en la Fiscalía General de la República con sede en San Miguel, las herramientas jurídicas, se auxilian de la Ley Especial contra los Delitos

Informáticos y Conexos y además tienen preestablecidos los procedimientos en el Código Procesal Penal, en el sentido que ya están determinados los parámetros para dirigir la investigación; sin embargo, no son la únicas herramientas que existen para tratar los delitos informáticos, ya que también se apoyan en la Sección de Análisis y Tratamiento de Información (SATI) de la Policía Nacional de Civil y la Dirección de Análisis Técnicas de Investigación e Información (DATI), que es una institución adscrita a la Fiscalía, y apoya en la gestión para obtener respuesta en todo lo relacionado a aspectos de tecnologías de la información y comunicación.

No se pudo tener acceso a la unidad especializada de la sede central en la FGR-La Sultana, a pesar de los diversos intentos y de los medios formales, que se presentaron, debido a la emergencia nacional por Covid-19, carga laboral, y por el tipo de información que se considera de carácter delicado. Se pudo acceder a información de la Unidad especializada de la PNC, por medio de la División Central de Investigaciones, a través de la Unidad de Acceso a la Información Pública; no obstante, se denegó la información sobre el tipo de herramientas tecnológicas científicas que utilizan para la investigación, por ser información de carácter reservado. Anexo 2, apartado 5 “Fundamento de la Reserva”

En la ciudad de San Miguel, es evidente que existen limitaciones *en la investigación* de los delitos informáticos de la LEDIC, y por tanto en el Delito de Revelación de Datos o Información de Carácter Personal, porque no existe una unidad especializada, ni medios materiales como herramientas especiales, ni protocolos que den los lineamientos idóneos para la investigación del Delito; por tanto, existe impunidad en la *investigación de este delito*, debido a que la mayoría de casos se archivan tanto en la Policía como en la Fiscalía.

De igual forma, en el período establecido para la investigación de este proyecto, de enero de 2018 a febrero de 2020, no se encontró mediante investigación de campo realizada a la PNC y FGR, ni los datos estadísticos, registrados en las bases de datos de las mencionadas instituciones que sustenten que se requirió formalmente un dictamen de acusación en el Delito de Revelación Indebida de Datos o Información de Carácter Personal, tampoco un caso

judicializado en condena o absolución.

Lo anterior lleva a plantearse que no existe una claridad en la investigación del delito de Revelación Indebida de Datos o Información de Carácter Personal y que no se le da la importancia debida, denotándose que existe un desinterés en establecer una investigación idónea para la identificación del sujeto activo que comete el ilícito penal. No se percibe un interés de parte de estas instituciones en dar una respuesta efectiva o esclarecer la investigación en el delito de Revelación Indebida de Datos o Información de Carácter Personal.

Cabe mencionar que el país cuenta con una Unidad para tratar este tipo de delitos, que surge a raíz de la creación de la Ley, como ya se ha mencionado, tal Unidad está conformada por personal idóneo altamente capacitado dentro y fuera del país, que poseen herramientas tecnológicas y científicas como son móviles, dispositivos y software especializados para el rastreo, seguimiento y finalización de la investigación; sin embargo, la Unidad se haya centralizada en la sede de San Salvador de la PNC, y se constituye el único medio de auxilio para todas las unidades de investigación del país.

5.2 RECOMENDACIONES.

a) Fortalecer las Unidades de Investigación de este tipo de delitos, tecnificando y dotando de personal capacitado y las herramientas tecnológicas necesarias para de indagación de los hechos y la identificación de los responsables de los mismos.

b) Que haya contratación de recursos humanos en todas las sedes del departamento de investigación de la PNC, que cuenten con las competencias tecnológicas, intelectuales, físicas y psicológicas, de acuerdo a las exigencias de la Ley, para en primera instancia, facilitar los procedimientos de investigación y apoyar a la unidad central especializada y reducir el hecho que la central continúe apoyando a las del interior del

país.

c) Lograr a mediano plazo, la creación de nuevas unidades especializadas en la zona oriental y occidental del país, con el objetivo de reducir la impunidad *en la investigación* del cometimiento de los delitos informáticos, en especial del Delito de Revelación Indebida de Datos o Información de Carácter Personal, por la razón, de ser el más cometido, para que se comience a perfilar la investigación, debiendo llevar a la par del avance de la tecnología de la comunicación y la mejora continua del equipo especializado.

d) En cuanto a la capacitación y formación constantes, que sea para todas las sedes policiales y propiciar oportunidades para que haya acceso dentro de la carrera policial, a una especialización en la LEDIC.

e) Que El Salvador, seleccione países de primer mundo que contenga una alta especialización en la investigación de la ciberdelincuencia y así establecer acuerdos y convenios con ellos, y podría optar a que forme parte del convenio de Budapest.

f) Que se establezca un ciber-patrullaje rutinario para controlar los hechos cometidos a través del mal uso de las herramientas que la ciberdelincuencia utiliza para operar.

GLOSARIO

- **Ciberdelito.** Es un término genérico que hace referencia a la actividad delictiva de las acciones en internet o relacionadas, llevada a cabo mediante equipos informáticos o a través de internet. El ciberdelito puede hacer uso de diferentes métodos y herramientas, con el objetivo de robar información personal o de realizar actividades fraudulentas (Intelectual Abogados, 2019)

- **Crime-as-a-service**. El Crime as a service es una tendencia en auge. Es el denominado crimen como servicio (Crime as a service o CaaS) que hace referencia a criminales que ofrecen sus servicios a cualquier persona/entidad que quiera pagarlos: entrar en la cuenta de Facebook de otra persona, espiar WhatsApp, insertar malware, obtener credenciales de acceso, interceptar correos. Son solo algunos ejemplos sencillos, pero no hay límite a lo que se puede conseguir mediante la contratación de estos «servicios» ilegales especiales (Eitzen, 2018)

- **Darkenet.** Es una colección de redes y tecnologías utilizadas para compartir contenido digital. La darknet no es una red física separada, sino una aplicación y una capa de protocolo que se monta en las redes existentes. Ejemplos de redes oscuras son el intercambio de archivos entre pares, la copia de CD y DVD y el intercambio de claves o contraseñas en el correo electrónico y los grupos de noticias (Biddle P., 2003)

- **Delito cibernético.** Así como la computadora se presenta como una herramienta muy favorable para la sociedad, también se puede convertir en un instrumento u objeto en la comisión de verdaderos actos ilícitos. Dependiendo de su tipificación o no, los delitos cibernéticos son “actitudes ilícitas en que se tiene a la Cibernética

como instrumento o fin" (concepto atípico) o las "conductas típicas, antijurídicas y culpables en que se tiene a la Cibernética como instrumento o fin" (Valdéz, 1998)

- **Ransomware.** Es un programa de software malicioso que infecta la computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema. Este tipo de malware, es un sistema criminal para ganar dinero que se puede instalar a través de enlaces engañosos, incluidos en un mensaje de correo electrónico, mensaje instantáneo o sitio web. El ransomware tiene la capacidad de bloquear la pantalla de una computadora o cifrar archivos importantes predeterminados con una contraseña. (Kaspersky, 2020)
- **SIGLAS**
    - **DATI.** Dirección de Análisis, Técnicas de Investigación e Información
    - **DCI:** División Central de Investigaciones
    - **D L.** Decreto Legislativo
    - **D O.** Diario Oficial
    - **FGR.** Fiscalía General de la República
    - **OEA.** Organización de Estados Americanos.
    - **LACNIC.** Es una organización no gubernamental internacional, encargada de establecer el Registro de Direcciones de Internet de América Latina y Caribe, que asigna y administra los recursos de numeración de Internet (IPv4, IPV6)
    - **PNC.** Policía Nacional Civil.
    - **REMJA**. Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas.

- **SATI**. Sección de Análisis y Tratamiento de la Información (Policía Nacional Civil)
- **SIGAP**. Sistema de Información y Gestión Automatizada del Proceso Fiscal.
- **TICs.** Tecnologías de la Información y la Comunicación.
- **UAIP.** Unidad de Acceso a la Información Pública
- **UNODC**. Oficina de las Naciones Unidas contra la Droga y el Delito.

BIBLIOGRAFÍA

Arrocena, G. (2011). La regulación de los delitos informáticos en el código penal argentino. *Boletín mexicano de Derecho Comparado*(135), 945-988.

Biddle P., E. P. (2003). *Gestión de derechos digitales. DRM 2002.* Obtenido de The Darknet and the Future of Content Protection. : https://link.springer.com/chapter/10.1007/978-3-540-44993-5_10#citeas

Eitzen, C. D. (4 de Noviembre de 2018). *Blog de Christian DvE (Beta)*. Obtenido de http://www.christiandve.com/2018/11/que-es-crimen-como-servicio-crime-as-a-service-caas/

ESET Security Report, Latinoamérica. (2015). Obtenido de https://www.welivesecurity.com/wp-content/uploads/2015/03/ESET_security_report_2015.pdf

Feusier, & Martínez. (s.f.). Concurso de investigación CNJ. *Aplicación y contenido de la Ley Especial contra la delincuencia informática y conexos*, p. 66-67. San Salvador, San Salvador, El Salvador. Obtenido de academia.edu/41596209/APLICACIÓN_Y_CONTENIDO_DE_LA_LEY_ESPECIAL CONTRA_LA_DELINCUENCIA_INFORMÁTICA_Y_CONEXOS_CONCURSO_ DE_INVESTIGACIÓN_CNJ_Fomentando_la_investigación_para_mejorar_la_ Administración_de_Justicia_

Flores Prada, I. (2012). *Criminalidad Informáticas. Aspectos sustantivos y procesales.* Valencia, España: Editorial Tirant lo Blanch.

Gutiérrez, M. E. (julio de 1994). *Habeas Data [monografía Licenciatura en Ciencias Jurídicas, Universidad Salvadoreña Alberto Masferrer].* Repositorio Institucional, San Salvador, San Salvador, El Salvador. Obtenido de http://www.csj.gob.sv/BVirtual.nsf/3db6532d39e032fd06256b3e006d8a73/cd419dec2640ca0f06256b3e00747d3d?OpenDocument.

Hernández Díaz, L. (2010). *Aproximación a un concepto de derecho penal informático. En derecho penal informático.* Civitas, España.

IAIP. (Noviembre de 2018). 1 Serie de cuadernos de transparencia. Cuaderno de sistematización de datos personales en el IAIP. *Sistematización de casos sobre protección de datos personales en el IAIP*. San Salvador, San Salvador, El Salvador.

Iberoamericana, Grupo E-Justicia Cumbre Judicial. (Abril de 2018). Compendio Normativo Sobre Ciberdelincuencia. *XIX Edición-Cumbre Judicial Iberoamericana*. Ecuador.

Inconstitucionalidad , 58-2007 (Sala de lo Constitucional 8 de marzo de 2013).

Inconstitucionalidad, Ley de Partidos Políticos, 35-2016 (Sala de lo Constitucional de la Corte Suprema de Justicia de El Salvador 12 de mayo de 2017).

Intelectual Abogados. (2019). Obtenido de https://intelectualabogados.com/delitos-informaticos-ciberdelitos-y-delitos-en-redes-sociales/que-es-el-ciberdelito/#:~:text=El%20ciberdelito%20es%20un%20t%C3%A9rmino, inform%C3%A1ticos%20o%20a%20trav%C3%A9s%20de%20Internet.&text= El%20ciberdelito%20es%20en.

Kaspersky, E. (2020). *Kaspersky.* Obtenido de https://latam.kaspersky.com/ resource-center/definitions/what-is-ransomware.

LACNIC. (s.f.). *LACNIC*. Obtenido de https://www.lacnic.net/966/1/lacnic/acerca-de-lacnic

LEDIC. (26 de febrero de 2016). *Ley Especial contra delitos informáticos y conexos*. San Salvador, San Salvador, El Salvador.

LINARES, O. C., & SEVILLANO FLORES, J. A. (s.f.). *UNIVERSIDAD DON BOSCO DE EL SALVADOR. Obtenido de http://*

rd.udb.edu.sv:8080/jspui/bitstream/11715/958/1/TESIS_DESAF%C3%8DDOS_APLICACI%C3%93N_LEYES_DELITOS_INFORM%C3%81TICOS_EL_SALVADOR_1.pdf

Northon Ciberseguridad. (Recuperado 30-mayo-2017 de 2016). Obtenido de https://www.symantec.com/content/dam/symantec/mx/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf

OEA. (2016). *OEA.* (D. d. Prensa, Ed.) Obtenido de https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-063/16

Paris, M. (28 de marzo de 2016). *2020 Observatorio Iberoamericano de Protección de Datos.* Obtenido de http://oiprodat.com/2016/03/28/nueva-ley-de-delitos-informaticos-de-el-salvador/

Pérez Luño, A. E. (1984). *Derechos Humanos, Estado de Derecho y Constitución.* Madrid: Tecnos.

SALVADOR, U. E. (uno de Julio de 2020). Solicitud N°151-UAIP-FGR-2020. San Salvador, San Salvador, El Salvador.

UNODC. (2020). *UNODC.org Centroamérica y el Caribe*. Obtenido de wwwwww.unodc.org>cybercrime-training-in-el-salvador: https://www.unodc.org/ropan/es/IndexArticles/Cybercrime/cybercrime-training-in-el-salvador.html

UNODC Centroamérica y el Caribe. (2016). *Policía Nacional de El Salvador fortalece sus capacidades en la investigación de delitos cibernéticos*. Obtenido de UNODC Centroamérica y el Caribe: https://www.unodc.org/ropan/es/IndexArticles/Cybercrime/cybercrime-training-in-el-salvador.html

UNODC Centroamérica y el Caribe. (julio de 2016). *UNODC, Continúa Fortaleciendo las Capacidades de El Salvador en la Lucha Contra el Cibercrimen*. Obtenido de UNODC Centroamérica y el Caribe: https://www.unodc.org/ropan/es/

unodc--continua-fortaleciendo-las-capacidades-de-el-salvador-en-la-lucha-contra-el-cibercrimen.html

UNODC ROPAN. (2018). *www.unodc.org/ropan*. Obtenido de http:// escuela.fgr.gob.sv/wp-content/uploads/leyes-nuevas/analisis-juridico-de-la-ley-especial-contra-los-delitos-informaticos-y-conexos-COMPLETO-CAP-I-II-III-V.pdf

Valdéz, J. T. (1998). *Informática y Derecho.* Ciudad de México: dialnet.unirioja.es.

ANEXOS

Anexo 1. Policía Nacional Civil. Resolución final ref. C-210-2019

POLICIA NACIONAL CIVIL
Resolución de Final ref. C – 210 – 2019.

EN LA UNIDAD DE ACCESO A LA INFORMACION PUBLICA, DE LA POLICIA NACIONAL CIVIL, UBICADA EN LA SEXTA CALLE ORIENTE NUMERO CUARENTA Y DOS, ENTRE OCTAVA Y DECIMA AVENIDA SUR, BARRIO LA VEGA; SAN SALVADOR, A LAS OCHO HORAS DEL DIA CUATRO DE MAYO AÑO DOS MIL VEINTE. HABIENDO RECIBIDO LA SOLICITUD POR EL CIUDADANO **HECTOR DAVID ARGUETA GRANADOS,** SE ANALIZÓ Y DETERMINÓ QUE EL REFERIDO DOCUMENTO REÚNE LOS REQUISITOS ESTABLECIDOS EN EL ARTÍCULO SESENTA Y SEIS DE LA LEY DE ACCESO A LA INFORMACIÓN PUBLICA, POR LO QUE SE ADMITE Y REGISTRA CON EL NÚMERO DE REFERENCIA PNC–UAIP–210 – 2020.

DETALLE DE LA INFORMACION SOLICITADA:

1. Cual delito es el más denunciado.
2. Cantidad de denunciado.
3. Números de casos investigados.
4. Números de casos que están en investigación.
5. Cuantos casos investigados han sido puestos a la disposición de la fiscalía.
6. Técnicas y herramientas que utilizan para investigación, especificamente en los delitos de REVELACIÓN INDEBIDA DE DATOS O INFORMACIÓN DE CARACTAER PERSONAL.

En base a lo establecido en el Artículo cincuenta y cinco del Reglamento de la Ley de Acceso a la Información Pública, se procedió a solicitar la información requerida a las Unidades Administrativas correspondientes (**DELEGACIÓN SAN MIGUEL Y DIVISIÓN CENTRAL DE INVESTIGACIÓN**).

CONSIDERANDO: que la información solicitada en los requerimientos a y b no se encuentran clasificada entre las excepciones señaladas en los artículos diecinueve y veinticuatro de la Ley de Acceso la Información pública, y que el Art. 62 de la Ley de Acceso la Información pública, determina """ **Los entes obligados deberán entregar en su poder.** **RESUELVO:** BRINDAR RESPUESTA a la información requerida por el solicitante en formato digital, de los puntos 1 al 5 en forma completa.

DENEGAR El PUNTO 6, este tipo de información está clasificado como reservado de acuerdo al DCI – 003 – 2018.

El fundamento de esta denegatoria está basado en el (memorándum SIN/DCI/0232/2020 de fecha 16 de ABRIL de 2020 suscrito por el Jefe de la dependencia antes mencionada.

De conformidad a lo señalado en el Art. 82 de la Ley de Acceso a la Información Pública, se informa al solicitante que dispone del recurso de apelación a la presente resolución, el cual puede interponer en esta Unidad o ante el Instituto de Acceso a la Información Pública, ubicado en: **Prolongación Avenida Mas Ferrer, Calle al volcán #88, edificio Oca Chang, San Salvador. –Teléfono: 2205-3800 – Telefax: 22053880 y correo electrónico: oficialreceptor@iap.gob.sv**

No habiendo más que hacer constar, firmo y sello la presente resolución la cual notifico al solicitante de forma personal.

COMISIONADO LUIS ERNESTO NUÑEZ CARCAMO.
OFICIAL DE INFORMACIÓN

Cabezas

2

Anexo 2. Policia Nacional Civil. Memorandum. SIN/DCI/0232/2020

DIVISIÓN CENTRAL DE INVESTIGACIONES

GOBIERNO DE EL SALVADOR

MINISTERIO DE JUSTICIA Y SEGURIDAD PÚBLICA

DIRECCIÓN GENERAL
UNIDAD DE ACCESO A LA INFORMACIÓN
POLICÍA NACIONAL CIVIL
20 ABR. 2020
RECIBE:
HORA: 10:43

MEMORÁNDUM

SIN/DCI/ [redacted] -0232 /2020

PARA : COMISIONADO LUIS ERNESTO NUÑEZ CÁRCAMO
OFICIAL DE INFORMACIÓN

DE : COMISIONADO DOUGLAS ELENILSON ZOMETA
JEFE DIVISIÓN CENTRAL DE INVESTIGACIONES

ASUNTO : CONTESTANDO MM433

FECHA : SAN SALVADOR, 16 DE ABRIL DE 2020

POLICÍA NACIONAL CIVIL DE EL SALVADOR
DCI
JEFATURA

Respetuosamente y en atención a su memorándum No.PNC/UAIP/433/2020, en el cual informa que ha recibido solicitud de una persona cuyo nombre se omite por razones quien ha solicitado la información pública que se detalla a continuación:

DETALLE DE LA INFORMACIÓN SOLICITADA:

Detallando información de datos estadísticos sobre los delitos informáticos en la Policía Nacional Civil, con sede en la Ciudad de San Miguel:

1. Cuál delito es el más denunciado.
2. Cantidad de denunciado.
3. Números de casos investigados.
4. Números de casos que están en investigación.
5. Cuántos casos investigados han sido puestos a la disposición de la fiscalía.
6. Técnicas y herramientas que utilizan para investigación, específicamente en los delitos de REVELACIÓN INDEBIDA DE DATOS O INFORMACIÓN DE CARÁCTER PERSONAL.

En razón de lo anterior se remite en formato Excel, las respuestas de los numerales 1 y 2, no así de las interrogantes de la 3 a la 5, por corresponderle al Departamento de Investigación Territorial.

En relación al numeral 6, este tipo de información está clasificada como RESERVADA.

Sin nada más que agregar, me despido de usted.
DEZ/vpc.

Colonia Flor Blanca, Calle El Progreso No. 2810, contiguo Edificio Post Grado UFG, San Salvador
Fax: 2511-1479 Teléfonos 2511-1463 y 2511-1452

POLICIA NACIONAL CIVIL
SUBDIRECCION DE INVESTIGACIONES

ACTO ADMINISTRATIVO INFORMACION DE RESERVA DE LA SUBDIRECCION DE INVESTIGACIONES

1.0 Tema:

Casos de investigación nacional y transnacional; así como también la elaboración de Peritajes por parte de la División de Policía Técnica y Científica, con sus respectivos resultados.-

2.0 Fecha de Reserva de la Información:

05 septiembre de 2016.

3.0 Fuentes productoras de la Información:

Subdirección de Investigaciones

1. División Central de Investigaciones (DCI)
2. División Elite Contra el Crimen Organizado (DECO)
3. División Antinarcóticos (DAN)
4. División de Investigación Patrimonial de Extinción de Dominios y Delitos Financieros (DIPEDDF)
5. División Policía Técnica y Científica (DPTC)
6. División de Investigación Criminal Transnacional (DICT)
7. División Antiextorsiones (DIE)
8. División Antipandillas (DIA)
9. Centro Antipandillas Transnacional (CAT)
10. Oficinal Regional INTERPOL El Salvador
11. Unidad Central de Análisis y Tratamiento de la Información (UCATI)
12. Departamentos de investigaciones en Delegaciones Policiales (DIN)

4.0 Plazo de Reserva:

Con base en los artículos 75 Atribuciones de la Investigación, 76 Publicidad de las actividades de la investigación, 260 al 274 todos del Código Procesal Penal (Pr.Pn.) en relación a con el artículo 20 de LAIP, se establecerá como plazo el tiempo que dure la investigación técnica y jurídica, hasta su finalización ya sea en vista pública o en casación penal. Asimismo, el Art. 72 de la Ley Reguladora de las Actividades Relativas a las Drogas, establece que durante las diligencias iniciales de investigación y por la naturaleza de los delitos que le corresponden investigar, las actuaciones de la División Antinarcóticos y de la Fiscalía General de la República serán reservadas.

Los casos investigados por la Subdirección de Investigaciones, se encuentran bajo la dirección funcional de la FGR, quien es el responsable de los expedientes investigativos hasta llegar a la fase judicial, con base al Artículo 193 numeral 3 de la Cn.

5.0 Fundamento de la Reserva:

Fundamento jurídico de la declaratoria de reserva de información

La Policía Nacional Civil de el Salvador, desde su creación constitucional con base en el artículo 159 inciso 3° específicamente la "Colaboración en el procedimiento de investigación ..." institución perteneciente del estado, quien por ministerio de ley, le corresponde trabajar con eficiencia, transparencia, eficacia y permanencia en su servicio, así como también en la colaboración con la FGR en la investigación del delito, con la función de Policía de Investigación, función conferida dentro de la corporación policial a la Subdirección de Investigaciones, como se encuentra previamente establecido en la Ley Orgánica de la Policía Nacional Civil Artículo 4

POLICIA NACIONAL CIVIL
SUBDIRECCION DE INVESTIGACIONES

Funciones de la Policía numeral 1, 4 y 5 y del Reglamento de la LOPNC en concordancia con los artículos 260 al 274 del Pr.Pn.

- En ese sentido se pondera que la información contenida en los casos de investigación nacionales y transnacionales iniciados por las dependencias adscritas a esta Subdirección, sean clasificados bajo la figura legal de INFORMACION RESERVADA, tomando como base lo establecido en los artículos 19 literales b, d, f y h, y 21 de la Ley de Acceso a la Información Publica abreviado LAIP, en concordancia con el mandato constitucional del Artículo 2. Así también atendiendo a los criterios últimamente incorporados por los miembros del Instituto de Acceso a la Información que se refieren a los criterios de Prejudicialidad es procedente que los casos de inicio de investigación sean direccionados por la FGR quien direccione o no su judicialización.

Por otra parte es de tomar en cuenta que la información contenida en los casos de investigación, es información indiciaria no certera que pueda servir de base para una aseveración, asimismo en ella está contenida información con datos de personas de las que no se cuenta con el asentimiento de divulgar sus generales, y la Policía de Investigación está en la obligación de salvaguardar la vida e integridad de las personas que podrían tener la calidad de víctima, testigo e imputado, por lo que se anteponen sus derechos fundamentales con el derecho de acceso a la información; tomando como base constitucional el artículo 2 de la Cn., relacionados con los artículos 105 y 106 calidad de víctima y derechos de la víctima del Pr.Pn, estas disposiciones constitucionales se refieren que la PNC como operador público está en la obligación de proteger y salvaguardar los derechos que le confieren a las personas que tienen calidad de víctimas; asimismo en los artículos 11 (Principio de única persecución y Juicio Previo) y art. 12 (Principio de inocencia o culpabilidad y juicio oral) de la Constitución de la República en relación con el artículo 82 (Derechos del imputado) del Pr.Pn, las personas que están señaladas o se les atribuye un delito o falta penal, también la Policía de Investigación está en la

POLICIA NACIONAL CIVIL
SUBDIRECCION DE INVESTIGACIONES

obligación de salvaguardar sus derechos Constitucionales y procesales, es por eso se hace necesario la clasificación de información bajo la modalidad de reservada.

Las disposiciones procesales contempladas en los artículos 260 al 274 del Pr.Pn., dichas se refieren a los actos iniciales de investigación, función conferida a la Policía de Investigación, aunado a eso se tiene la definición doctrinaria de la **Sala de lo Penal de la Corte Suprema de Justicia en diversas líneas jurisprudenciales "Como aquellos actos de investigación que tiene como objeto recoger los elementos de prueba que serán utilizados para verificar la propuesta de las partes durante el juicio y justificar el grado de probabilidad, las resoluciones que dictara el Juez; es decir que la finalidad es obtener, identificar o asegurar las fuentes de información que proporciones la elaboración de respuesta coherentes sobre la ejecución de un hecho delictivo y su presunto autor (723 CAS/2011)".**

La Subdirección de Investigaciones con base en los artículos 174(finalidad de la prueba) y 226 ordinal b (Nombramiento de peritos) del Pr.Pn., por medio de la División de Policía Técnica y Científica, le corresponde realizar peritajes que forman parte de la investigación policial, mismas que son utilizadas por las partes (Fiscalía y Defensa); y así como también de manera eventual al justiciable en los procesos de ubicación, recolección y utilización de los medios de convicción que servirán como medios de prueba de una eventual vista pública.

La Subdirección de Investigaciones, le corresponde además de los otros casos ya mencionados aplicar la reserva de información en los casos contemplados en el artículo 327 Otros casos de aprehensión del Pr.Pn., en razón de los fundamentos constitucionales ya mencionados se tiene que también salvaguardar la vida, la integridad de las personas en los casos de personas con difusión o circular roja de Instituciones policiales internacionales con la cual se realiza otro tipo de procedimientos.

POLICIA NACIONAL CIVIL
SUBDIRECCION DE INVESTIGACIONES

De lo anterior es necesario acotar y hacer un razonamiento y juicio lógico que nos permita determinar que ante el conflicto, debemos buscar una valoración en el ejercicio de ambos derechos fundamentales (vida, integridad, otros y acceso a la información) y si esto no es posible, uno debe ceder frente el otro, puesto que en el caso concreto no pueden ser satisfechos simultáneamente, no constituyendo lo anterior el sacrificio de un derecho por la adopción de otro, esto viene a confirmar que, los derechos fundamentales no son absolutos, pueden verse limitados en circunstancias particulares como las que se señalan, en tal sentido la limitación del derecho de acceso a la información relacionada, implica una limitación en cuanto al ejercicio práctico del derecho y no en cuanto a su esencia, pues frente al derecho de acceso a la información, existe otro derecho fundamental que posee mayor relevancia como el derecho a la vida y la integridad física, en otras palabras el daño que produciría la liberación de la información que se está reservando es mayor que el interés público por conocerla.

Por lo tanto resuelvo en mi calidad de Subdirector de Investigaciones, según acuerdo No. A-0248-03-2016, firmado por el señor Director General, reservar la información generada por las Divisiones y Unidades adscritas a esta Subdirección, según los párrafos arriba mencionados. San salvador a los cinco días del mes de septiembre de 2016.

6.0 Autoridad que adopta la decisión de Reserva de Información:

F.

Comisionado Juan Carlos Martínez Marín
Subdirector de Investigaciones

Anexo 3. Datos Estadísticos Delitos en la Ciudad de San Miguel 01 enero-31 diciembre 2019

LOS DATOS CORRESPONDEN A LA CIUDAD DE SAN MIGUEL EN EL PERIODO COMPRENDIDO DEL 01 DE ENERO AL 31 DE DICIEMBRE DE 2019

DELITOS	FACEBOOK	FACEBOOK, INSTAGRAN	FACEBOOK, INTERNET	FACEBOOK, INTERNET, VK	FACEBOOK, VK	FACEBOOK, WHATSAPP	FACEBOOK, WHATSAPP, INTENET	INTERNET	INTERNET, VK	TWITTER	VK	WHATSAPP	WHATSAPP, INTERNET	WHATSAPP, VK	REDES SOCIALES	TOTAL GENERAL
AMENAZAS	14					4		7				10			1	36
ESTAFA	8							9				8	1			26
REVELACION INDEBIDA DE DATOS O INFORMACION DE CARACTER PERSONAL	14					1		6				1		1		23
DIFUSION ILEGAL DE INFORMACION	7				4			3			2	2			1	19
HURTO	3		1					2				5				11
PRIVACION DE LIBERTAD	4							1				5	1			11
UTILIZACION DE DATOS PERSONALES	4					1		2								7
EXPRESIONES DE VIOLENCIA CONTRA LA MUJER	3							2				1				6
DIFUSION DE PORNOGRAFIA	3			1				2								6
EXTORSION	1						1					3				5
ESTAFA AGRAVADA			1					1					2		1	5
HURTO DE IDENTIDAD	4									1						5
ACOSO DE NIÑAS, NIÑOS, ADOLESCENTES O PERSONAS CON DISCAPACIDAD A TRAVES DEL USO DE LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN	2	1							1						1	5
LESIONES	2							1				1				4
VIOLACION EN MENOR E INCAPAZ	3															3
EXTORSION AGRAVADA												3				3
FALSEDAD MATERIAL								3								3
AMENAZAS CON AGRAVACION ESPECIAL	2							1								3
VIOLENCIA INTRAFAMILIAR	1					1										2
HURTO DE VEHICULOS AUTOMOTORES	1							1								2
AGRESION SEXUAL EN MENOR E INCAPAZ	1							1								2
ESTAFA INFORMATICA	1					1										2
DAÑOS	1															1
APROPIACION O RETENCION INDEBIDAS												1				1
ACOSO SEXUAL												1				1
LIMITACION ILEGAL A LA LIBERTAD DE CIRCULACION	1															1
VIOLACION	1															1
TRAFICO ILEGAL DE PERSONAS						1										1
ROBO DE VEHICULOS AUTOMOTORES	1															1
USO Y TENENCIA DE DOCUMENTOS FALSOS								1								1
APROPIACION INDEBIDA DE VEHICULO AUTOMOTOR	1															1
LESIONES CULPOSAS												1				1
TRATA DE PERSONAS (19)	1															1
ESTUPRO	1															1
EXPRESIONES DE VIOLENCIA CONTRA LAS MUJERES	1															1
DELITOS EN LA LEY ESPECIAL CONTRA EL DELITO DE EXTORSION												1				1
LESIONES, ROBO	1															1
DIVULGACION NO AUTORIZADA											1					1
SECUESTRO	1															1
FRAUDE INFORMATICO	1															1
FALSEDAD MATERIAL, USO Y TENENCIA DE DOCUMENTOS FALSOS								1								1
PORNOGRAFIA A TRAVES DEL USO DE LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN								1								1
DELITOS RELATIVOS A LA FE PUBLICA								1								1
PRIVACION DE LIBERTAD AGRAVADA, VIOLACION	1															1
VEHICULO EXTRAVIADO C/PERSON												1				1
DIFUSION ILEGAL DE INFORMACION, EXPRESIONES DE VIOLENCIA CONTRA LA MUJER	1															1
ACOSO SEXUAL, REVELACION INDEBIDA DE DATOS O INFORMACION DE CARACTER PERSONAL								1								1
AMENAZAS, DIVULGACION NO AUTORIZADA															1	1
UTILIZACION DE NIÑAS, NIÑOS, ADOLESCENTES O PERSONAS CON DISCAPACIDAD EN PORNOGRAFIA A TRAVES DEL USO DE LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN															1	1
ACOSO SEXUAL, DISCRIMINACION LABORAL												1				1
TOTAL	91	1	2	1	4	9	1	47	1	1	3	45	4	1	6	217

Anexo 4. Datos Estadísticos Sobre Delitos Informáticos Años 2019-2020 - Unidad De Acceso a la Información Pública/ OIR-PNC

DATOS SOBRE DELITOS INFORMATICOS AÑOS 2019-2020

AÑO 2019

DELITO	CASOSINICIADOS	DENUNCIADOS	INVESTIGADOS	EN INVESTIGACION	DISPOSICION FGR
ACOSO DE NIÑAS, NIÑOS, ADOLESCENTES O PERSONAS CON DISCAPACIDAD A TRAVES DEL USO DE LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN	3	3		3	3
DIFUSION DE PORNOGRAFIA	7	7		7	7
DIFUSION ILEGAL DE INFORMACION	29	29		29	29
DIVULGACION DE LA IMAGEN O REVELACION DE DATOS DE PERSONAS PROTEGIDAS	2	2	1	1	2
FRAUDE INFORMATICO	1	1		1	1
HURTO POR MEDIOS INFORMATICOS	3	3		3	3
INDUCCION, PROMOCION Y FAVORECIMIENTO DE ACTOS SEXUALES O EROTICOS POR MEDIOS INFORMATICOS O ELECTRONICOS	1	1	1	0	1
MANIPULACION FRAUDULENTA DE TARJETAS INTELIGENTES	2	2	1	1	2
PORNOGRAFIA A TRAVES DEL USO DE LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN	1	1		1	1
REVELACION INDEBIDA DE DATOS O INFORMACION DE CARACTER PERSONAL	29	29	3	26	29
UTILIZACION DE NIÑAS, NIÑOS, ADOLESCENTES O PERSONAS CON DISCAPACIDAD EN PORNOGRAFIA A TRAVES DEL USO DE LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN	1	1		1	1
UTILIZACION DE NIÑOS Y NIÑAS EN PORNOGRAFIA ATRAVES DE LAS TECNOLOGIAS	1	1		1	1
Total general	**80**	**80**	**6**	**74**	**80**

AÑO 2020

DELITO	CASOSINICIADOS	DENUNCIADOS	INVESTIGADOS	EN INVESTIGACION	DISPOSICION FGR
ACCESO INDEBIDO A LOS PROGRAMAS O DATOS INFORMATICOS	1	1		1	1
DIFUSION ILEGAL DE INFORMACION	10	10		10	10
HURTO POR MEDIOS INFORMATICOS	1	1		1	1
INDUCCION, PROMOCION Y FAVORECIMIENTO DE ACTOS SEXUALES O EROTICOS	1	1		1	1
REVELACION INDEBIDA DE DATOS O INFORMACION DE CARACTER PERSONAL	11	11		11	11
Total general	**24**	**24**	**0**	**24**	**24**

Anexo 5. Datos Estadísticos: Cantidad de Casos Ingresados por los Delitos de la LEDIC en el Dpto. de San Miguel, en el Período de Enero de 2018 - Febrero 2020, Desagregado por Delito y Año.

CANTIDAD DE CASOS INGRESADOS POR LOS DELITOS DE LA LEY ESPECIAL CONTRA DELITOS INFORMATICOS Y CONEXOS SUCEDIDOS EN EL DEPARTAMENTO DE SAN MIGUEL EN EL PERIODO COMPRENDIDO DESDE EL MES DE ENERO DEL AÑO 2018 HASTA EL MES DE FEBRERO DEL AÑO 2020, DESAGREGADO POR DELITO Y AÑO.				
Delitos	**Año 2018**	**Año 2019**	**Año 2020**	**Total**
Acceso indebido a sistemas informáticos (4 L.D. Informáticos)	0	1	0	**1**
Acceso indebido a los programas o datos informáticos (5 L.D. Informáticos)	0	0	1	**1**
Violación de la seguridad de sistemas (9 L.D. Informáticos)	0	1	0	**1**
Estafa informática (10 L.D. Informáticos)	0	8	0	**8**
Fraude informático (11 L.D. Informáticos)	1	0	0	**1**
Hurto por medios informáticos (13 L.D. Informáticos)	3	6	2	**11**
Manipulación fraudulenta de tarjetas inteligentes o instrumentos similares (16 L.D. Informáticos)	4	3	0	**7**
Obtención indebida de bienes o servicios por medio de tarjetas inteligentes o medios similares (17 L.D. Informáticos)	2	1	0	**3**
Hurto de identidad (22 L.D. Informáticos)	2	7	2	**11**
Divulgación no autorizada (23 L.D. Informáticos)	0	2	0	**2**
Utilización de datos personales (24 L.D. Informáticos)	15	11	0	**26**
Obtención y transferencia de información de carácter confidencial (25 L.D. Informáticos)	1	0	0	**1**
Revelación indebida de datos o información de carácter personal (26 L.D. Informáticos)	11	35	9	**55**
Acoso a través de TIC (27 L.D. Informáticos)	1	0	0	**1**
Pornografía a través de TIC (28 L.D. Informáticos)	0	3	0	**3**
Utilización de NNA o personas con discapacidad en pornografía a través de las TIC (29 L.D. Informáticos)	0	5	0	**5**
Corrupción de NNA o personas con discapacidad a través del uso de las TIC (31 L.D. Informáticos)	1	0	0	**1**
Acoso a NNA o personas con discapacidad a través del uso de las TIC (32 L.D. Informáticos)	3	5	0	**8**
Corrupción de NNA o personas con discapacidad a través del uso de las TIC agravada (31 y 33 L.D. Informáticos)	0	1	0	**1**
Total	**44**	**89**	**14**	**147**

Fuente: Departamento de Estadística según registros de SIGAP a la fecha 25/06/2020
Nota: Los datos entregados corresponden a los casos iniciados en el periodo solicitado

Datos proporcionados por FGR/UAIP El Salvador (SALVADOR, 2020)

Anexo 6. Datos Estadísticos: Cantidad de Casos en Investigación Activa por los Delitos Contemplados en la LEDIC Registrados en el Departamento de San Miguel, en el Período de Enero de 2018 - Febrero 2020, Desagregado por Delito y Año.

CANTIDAD DE CASOS EN INVESTIGACIÓN ACTIVA POR LOS DELITOS CONTEMPLADOS EN LA LEY ESPECIAL CONTRA DELITOS INFORMATICOS Y CONEXOS REGISTRADOS EN EL DEPARTAMENTO DE SAN MIGUEL EN EL PERIODO COMPRENDIDO DESDE EL MES DE ENERO DEL AÑO 2018 HASTA EL MES DE FEBRERO DEL AÑO 2020, DESAGREGADO POR DELITO Y AÑO.				
Delitos	**Año 2018**	**Año 2019**	**Año 2020**	**Total**
Acceso indebido a sistemas informáticos (4 L.D. Informáticos)	0	1	0	**1**
Acceso indebido a los programas o datos informáticos (5 L.D. Informáticos)	0	0	1	**1**
Violación de la seguridad de sistemas (9 L.D. Informáticos)	0	1	0	**1**
Estafa informática (10 L.D. Informáticos)	0	5	0	**5**
Fraude informático (11 L.D. Informáticos)	1	0	0	**1**
Hurto por medios informáticos (13 L.D. Informáticos)	1	4	1	**6**
Manipulación fraudulenta de tarjetas inteligentes o instrumentos similares (16 L.D. Informáticos)	1	1	0	**2**
Obtención indebida de bienes o servicios por medio de tarjetas inteligentes o medios similares (17 L.D. Informáticos)	2	1	0	**3**
Hurto de identidad (22 L.D. Informáticos)	1	3	1	**5**
Divulgación no autorizada (23 L.D. Informáticos)	0	1	0	**1**
Utilización de datos personales (24 L.D. Informáticos)	2	1	0	**3**
Revelación indebida de datos o información de carácter personal (26 L.D. Informáticos)	5	23	8	**36**
Pornografía a través de TIC (28 L.D. Informáticos)	0	3	0	**3**
Utilización de NNA o personas con discapacidad en pornografía a través de las TIC (29 L.D. Informáticos)	0	5	0	**5**
Corrupción de NNA o personas con discapacidad a través del uso de las TIC (31 L.D. Informáticos)	1	0	0	**1**
Acoso a NNA o personas con discapacidad a través del uso de las TIC (32 L.D. Informáticos)	2	4	0	**6**
Corrupción de NNA o personas con discapacidad a través del uso de las TIC agravada (31 y 33 L.D. Informáticos)	0	1	0	**1**
Total	**16**	**54**	**11**	**81**

Fuente: Departamento de Estadística según registros de SIGAP a la fecha 25/06/2020
Nota: Los datos entregados corresponden a casos iniciados en el periodo solicitado que se encuentran en condición activa en Sede Fiscal.

Datos proporcionados por FGR/UAIP El Salvador (SALVADOR, 2020)

Anexo 7. Datos Estadísticos Sobre La Cantidad de Dictámenes por los Delitos de la LEDIC en el Dpto. de San Miguel, en el Período de Enero De 2018 - Febrero 2020.

CANTIDAD DE DICTAMENES ELABORADOS POR LOS DELITOS DE LA LEY ESPECIAL CONTRA DELITOS INFORMATICOS Y CONEXOS SUCEDIDOS EN EL DEPARTAMENTO DE SAN MIGUEL EN EL PERIODO COMPRENDIDO DESDE EL MES DE ENERO DEL AÑO 2018 HASTA EL MES DE FEBRERO DEL AÑO 2020, DESAGREGADO POR DELITO Y AÑO.	
Delitos	**Año 2018**
	*** Dictamen Fiscal (SES)**
Acceso indebido a los programas o datos informáticos (5 L.D. Informáticos)	1
Estafa informática (10 Lit. c. L.D. Informáticos)	1
Total	**2**

Fuente: Departamento de Estadística según registros de SIGAP a la fecha 25/06/2020
Nota: Los datos entregados son independientes a la fecha de inicio del caso.

7 151-UAIP-FGR-2020

Datos proporcionados por FGR/UAIP El Salvador (SALVADOR, 2020)

Anexo 8. Resolución Final 151-UAIP-FGR-2020

Fiscalía General de la República
Unidad de Acceso a la Información Pública

Solicitud Nº 151-UAIP-FGR-2020

FISCALÍA GENERAL DE LA REPÚBLICA, UNIDAD DE ACCESO A LA INFORMACIÓN PÚBLICA. San Salvador, a las catorce horas con diez minutos del día uno de julio de dos mil veinte.

Se recibió con fecha tres de abril del presente año, solicitud de información en el correo electrónico institucional de esta Unidad, conforme a la Ley de Acceso a la Información Pública (en adelante LAIP), enviada por el ciudadano **HÉCTOR DAVID ARGUETA GRANADOS**, con Documento Único de Identidad número cero tres millones seiscientos cuarenta y cinco mil quinientos setenta y tres guion ocho, de la que se hacen las siguientes **CONSIDERACIONES:**

I. En virtud de la Emergencia Nacional por la pandemia COVID-19, los términos y plazos procesales en los procedimientos administrativos y procesos judiciales, cualquiera que sea la materia y la instancia en que se encuentren, fueron suspendidos, conforme a lo siguiente: **Decreto Legislativo número 593,** de fecha 14 de marzo de 2020, publicado en el Diario Oficial N° 52, Tomo N° 426, de la misma fecha, en el que se decretó "ESTADO DE EMERGENCIA NACIONAL DE LA PANDEMIA POR COVID-19"; **Decreto Legislativo número 599,** del 20 de marzo de 2020, publicado en el Diario Oficial N° 58, Tomo N° 426; de la misma fecha en el cual se reformó el artículo 9 del Decreto Legislativo No. 593, de fecha 14 de marzo de 2020; **Decreto Legislativo número 622**, de fecha 12 de abril de 2020, publicado en el Diario Oficial N° 73, Tomo N° 427, de la misma fecha, en el cual se prorrogó la vigencia del Decreto Legislativo N° 593, de fecha 14 de marzo del año dos mil veinte, publicado en el Diario Oficial N° 52, Tomo N° 426, del 14 del mismo mes y año, y sus reformas posteriores, que contiene "ESTADO DE EMERGENCIA NACIONAL DE LA PANDEMIA POR COVID-19", por cuatro días; **Decreto Legislativo número 631,** del 16 de abril de 2020, publicado en el Diario Oficial N° 77, Tomo N° 427, de la misma fecha, en el cual se prorrogó la vigencia del Decreto Legislativo No. 593, de fecha 14 de marzo del año dos mil veinte, publicado en el Diario Oficial No. 52, Tomo No. 426, del 14 del mismo mes y año, y sus reformas posteriores, que contiene "ESTADO DE EMERGENCIA NACIONAL DE LA PANDEMIA POR COVID-19", por quince días; **Decreto Legislativo número 634,** del 30 de abril de 2020, publicado en el Diario Oficial N° 87, Tomo N° 427 de la misma fecha, en el cual se prorrogó la vigencia del Decreto Legislativo No. 593, de fecha 14 de marzo del año dos mil veinte, publicado en el Diario Oficial No. 52, Tomo No. 426, del 14 del mismo mes y año, y sus reformas posteriores, que contiene "ESTADO DE EMERGENCIA NACIONAL DE LA PANDEMIA POR COVID-19", por quince días; **Decreto Legislativo número 644** del 14 de mayo de 2020, publicado en el Diario Oficial N° 99, Tomo N° 427, de fecha 16 de mayo de 2020, en el que se decretó la Disposición Transitoria para la Ampliación de Plazos Judiciales y Administrativos en el Marco de la Ley de Regularización para el Aislamiento, Cuarentena, Observación y Vigilancia por COVID-19, por ocho días; **Resolución** de las dieciséis horas con treinta y seis minutos, del día 22 de mayo del presente año, dictada por la Honorable Sala de lo Constitucional, en la **Inconstitucionalidad 63-2020**, en la cual le dio nuevamente vigencia y hasta el 29 de mayo de 2020, al Decreto Legislativo número 593, de fecha 14 de marzo de 2020, publicado en el Diario Oficial N° 52, Tomo N° 426, de la misma fecha, en el que se

decretó Estado de Emergencia Nacional de la Pandemia por COVID-19; y el **Decreto Legislativo número 649,** del 31 de mayo del 2020, publicado en el Diario Oficial N° 111, Tomo N° 427, de fecha 01 de junio de 2020, en el que se Decretó la Suspensión de Plazos Procesales en los Procedimientos Administrativos y Procesos Judiciales, cualquiera que sea la materia y la instancia en la que se encuentren, debido a la Tormenta Tropical Amanda; razón por la cual, en esta fecha se está dando respuesta a su solicitud de información.

II. De la solicitud presentada, se tiene que el interesado literalmente pide se le proporcione la siguiente información:
"Solicito Información de datos estadísticos de delitos informáticos la Fiscalía General de la República, con sede en la ciudad de San Miguel:
1. Cual delito es el más denunciado por la población
2. Cantidad de denuncias
3. Número de casos investigados
4. Cantidad de requerimientos presentados
5. Técnicas y herramientas que utilizan para la investigación. Especificamente en el delito de REVELACIÓN INDEBIDA DE DATOS O INFORMACIÓN DE CARÁCTER PERSONAL."
Período Solicitado: Desde enero de 2028 hasta febrero de 2020.

III. Conforme a los artículos 66 LAIP, 72 y 163 inciso 1° de la Ley de Procedimientos Administrativos (en adelante LPA), se han analizado los requisitos de fondo y forma que debe cumplir la solicitud, verificando que ésta no cumple con los requisitos legales de claridad y precisión, por lo que, con la finalidad de dar respuesta a su solicitud, el día cinco de marzo del presente año se le solicitó que aclarara: *"1. En su solicitud cuando se refiere a **"delitos informáticos"**, debe especificar los delitos de los cuales requiere los datos estadísticos. Ya que la Fiscalía General de la República genera datos a partir de casos que ingresan por delitos específicos regulados en las leyes. Y el término utilizado es muy amplio. En el caso de referirse a los delitos regulados en la Ley Contra Delitos Informáticos y Conexos, debe especificar de cuales delitos de dicha ley especial solicita información o si requiere todos los delitos de dicha ley. 2. Así mismo, cuando dice **"denuncias"**, requiere especificamente solo este tipo de ingreso o todos los casos ingresados independientemente del medio de ingreso. 3.En su requerimiento cuando dice **"investigados"** debe especificar a qué se refiere, A fin de tener claridad de la información que solicita."*
El solicitante el día dieciséis de junio del corriente año, aclaró su solicitud de la siguiente manera: *"1. En su solicitud cuando se refiere a **"delitos informáticos"**, debe especificar los delitos de los cuales requiere los datos estadísticos. Ya que la Fiscalía General de la República genera datos a partir de casos que ingresan por delitos específicos regulados en las leyes. Y el término utilizado es muy amplio. En el caso de referirse a los delitos regulados en la Ley Contra Delitos Informáticos y Conexos, debe especificar de cuales delitos de dicha ley especial solicita información o si requiere todos los delitos de dicha ley. R/= Datos estadísticos de los delitos informáticos contemplados en la LEDIC (cuadro 1). CUADRO 1. Cantidad de Delitos de la LEDIC ingresados en la FGR, sede San Miguel.*

DELITOS DE LA LEDIC	***ENE-DIC 2018***	***ENE-DIC 2019***	***ENE-FEB 2020***
Acceso indebido a sistemas informáticos			
Acceso indebido a los programas o datos informáticos			
Interferencia del sistema informático			
Daño al sistema informático			
Posesión de equipo o prestación de servicios para la vulneración de la seguridad			
Violación de la seguridad de sistemas			
Estafa informática			

Estafa informática Art.10 literal "a"			
Estafa informática Art.10 literal "b"			
Estafa informática Art.10 literal "c"			
Fraude informático			
Espionaje informático			
Hurto por medio informático			
Técnicas de denegación de servicios			
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			
Alteración, daño a la integridad o disponibilidad de datos			
Interferencia de datos			
Intercepción de transmisiones entre sistemas de las TIC			
Hurto de identidad			
Divulgación no autorizada			
Utilización de datos personales			
Obtención y transferencia de información de carácter confidencial			
Revelación indebida de datos o información de carácter personal			
Acoso a través de TIC			
Acoso de NNA o personas con discapacidad a través del uso de las TIC			
Pornografía a través de las TIC agravada (28 y 33 L.D. Informáticos)			
Utilización de NNA o personas con discapacidad en pornografía a través de las TIC agravada (29 y 33 L.D. Informáticos)			
Corrupción de NNA o personas con discapacidad en pornografía a través de las TIC agravada (31 y 33 L.D. Informáticos)			
Acoso de NNA o personas con discapacidad en pornografía a través de las TIC agravada (32 y 33 L.D. Informáticos)			
Suplantación en actos de comercialización (34 L.D. Informáticos)			
Adquisición o posesión de material pornográfico de NNA o persona con discapacidad a través del uso de las TIC agravada			
TOTAL			

2. *Así mismo, cuando dice* ***"denuncias"****, requiere específicamente solo este tipo de ingreso o todos los casos ingresados independientemente del medio de ingreso. R/= Casos ingresados independientemente del medio de ingreso.*

3. *En su requerimiento cuando dice* ***"investigados"*** *debe especificar a qué se refiere. A fin de tener claridad de la información que solicita. R/= Envío el cuadro 2 con la información solicitada.*

CUADRO 2. Consolidado De Datos Estadísticos de La FGR Sede San Miguel, durante los períodos ene-dic2019, ene-dic 2019 y ene-feb 2020.

Número de casos ingresados			
Número de casos en que se requirió			
Número de casos en que se presentó dictamen			
Número de condenas logradas			
Número de absoluciones			
Número de casos en proceso			

Con la respuesta proporcionada y habiendo el interesado enviado copia de su Documento Único de Identidad, conforme a lo establecido en el artículo 52 del Reglamento LAIP, se continuó con el trámite de su solicitud.

IV. Con el objeto de localizar, verificar la clasificación y, en su caso, comunicar la manera en que se encuentra disponible la información, se transmitió la solicitud al Departamento de Estadística, de esta Fiscalía, conforme al artículo 70 LAIP.

V. De los requerimientos de información solicitados por el peticionario, se hace necesario realizar un análisis ordenando de los mismos a fin de darle respuesta a su petición y para efecto de fundamentar la decisión de este ente obligado, se procede de la siguiente forma:

a) Sobre el requerimiento número 5, que consiste en proporcionar las "*Técnicas y herramientas que utilizan para la investigación. Específicamente en el delito de Revelación Indebida de Datos o Información de Carácter Personal*; al realizar un análisis del mismo se puede colegir que el solicitante requiere se le brinden explicaciones sobre las diversas técnicas y herramientas utilizadas, tomando en cuenta que dichos términos son muy amplios, ya que existen infinidad de técnicas y herramientas que puedan utilizarse en las investigaciones criminales, esto conforme al Principio Procesal de Libertad Probatoria, establecido en el artículo 176 del Código Procesal Penal, los hechos que surjan de la investigación de cualquier delito pueden probarse por cualquier medio legal de prueba, tal como lo dispone el artículo antes señalado que establece: "*Los hechos y circunstancias relacionados con el delito podrán ser probados por cualquier medio de prueba establecido en este Código y en su defecto, de la manera que esté prevista la incorporación de pruebas similares, siempre que se respeten las garantías fundamentales de las personas consagradas en la Constitución y demás leyes.*".

b) Ante tal solicitud es determinante lo que dispone el Art. 1 LAIP, que define el objeto de la Ley, el cual consiste en garantizar el derecho de acceso de toda persona a la información pública, de lo cual se extrae que la LAIP regula el ejercicio pleno de acceso a la información pública; lo anterior se complementa con lo dispuesto en el Art. 2 LAIP, que dispone que toda persona tiene derecho a solicitar y recibir información generada, administrada o en poder de las instituciones públicas y demás entes obligados; en virtud de lo cual, la Fiscalía General de la República debe garantizarle a los ciudadanos el acceso a la información que genera, administra o tenga en su poder; esto se confirma con lo dispuesto en el Art. 6 Inc. 1º letra "c" LAIP, que expresa que se entiende como información pública aquella en poder de los entes obligados contenida en documentos, archivos, datos, bases de datos, comunicaciones y todo tipo de registros que documenten el ejercicio de sus facultades o actividades, que consten en cualquier medio, ya sea impreso, óptico o electrónico, independientemente de su fuente, fecha de elaboración, y que no sea confidencial; además, que dicha información podrá haber sido generada, obtenida, transformada o conservada por éstos a cualquier título.

c) Razón por la cual, este requerimiento de información solicitado por el peticionario no es factible de proporcionarlo, ya que requieren de una explicación en relación a temas concretos sobre el desarrollo de las investigaciones, en virtud que cada caso tiene sus particularidades en el desarrollo de la investigación, lo que puede conllevar a que en algunos casos se utilicen

diversas técnicas y herramientas y en otros no. En ese sentido, lo peticionado está fuera del alcance de la LAIP, ya que la generación de dichas explicaciones, implica la creación de información que existirá al momento de elaborar el documento, ya que dichas explicaciones pueden variar en casos concretos, razón por la que la petición de información del solicitante, está fuera del alcance de aplicación de la LAIP. Sobre este punto, el Instituto de Acceso a la Información Pública mediante resolución de referencia NUE 113-A-2016, de fecha veintitrés de mayo de dos mil dieciséis, ha señalado lo siguiente: *"...este Instituto aclara, que los procedimientos de acceso a la información pública sustanciados por las Unidades de Acceso a la Información Pública, son para acceder a información generada, administrada o en poder de los entes obligados (Art. 2 de la LAIP), no así para generar información."*

d) En razón de lo anterior, de conformidad con el literal c) del artículo 50 LAIP, que establece: *"Auxiliar a los particulares en la elaboración de solicitudes y, en su caso, orientarlos sobre las dependencias o entidades que pudieran tener la información que solicitan."*, se hace de conocimiento a la solicitante, que la Fiscalía General de la República cuenta con un servicio de entrevista, por medio del cual el tipo de información requerida puede ser accedida por una vía diferente a la LAIP, ya que se cuenta con un enlace institucional por el que las personas pueden acceder a información aún no generada por este ente obligado; en tal sentido, el interesado puede comunicarse al Departamento de Comunicación Interna de la Fiscalía General de la República, ubicado en Bulevard y Colonia La Sultana, Edificio G-12, Antiguo Cuscatlán, llamando a los teléfonos números 2593-7091, 2593-7000 y 2593-7001, y se le informen los pasos que debe seguir a fin de dirigir su petición a dicho Departamento y gestionar una entrevista con un servidor público conocedor del tema y de esa forma acceder a la información requerida.

e) En ese orden de ideas y por todo lo antes relacionado, es procedente entregar al solicitante la información de los numerales 1, 2, 3 y 4, siendo que la misma es la que es generada por esta Institución y tiene el carácter de pública, ya que no se encuentra dentro de ninguna de las causales de reserva previstas en el artículo 19 LAIP, y tampoco es información considerada confidencial de acuerdo a lo establecido en el Art. 24 LAIP.

POR TANTO, en razón de lo anterior, con base en los artículos 50 literales "b" y "c", 62, 65, 66, 71 y 72 todos de la LAIP y 163 inciso 1° LPA, se **RESUELVE:**

A) REORIENTAR, al peticionario para que pueda acceder a la información sobre las *"Técnicas y herramientas que utilizan para la investigación. Específicamente en el delito de revelación indebida de datos o información de carácter personal*, de la manera en que le ha sido expresado en el Romano V, literal d), de la presente resolución.

B) CONCEDER EL ACCESO A LA INFORMACIÓN, respecto a los requerimientos 1, 2,3 y 4, por medio de las siguientes respuestas:

1. **CUAL DELITO ES EL MÁS DENUNCIADO POR LA POBLACIÓN.**
R/ Respecto a este requerimiento de información, consistente en que se proporcione *"Cual es el delito más denunciado por la población"*, la información que se entrega corresponde a la Cantidad de casos ingresados por los delitos regulados en la Ley Especial Contra los delitos Informativos y Conexos, sucedidos en San Miguel, en virtud que no es posible proporcionarla tal como lo solicita, debido a que no se tiene ese nivel de sistematización en nuestra base de datos Institucional, sin embargo, dicha información pueda observarse en los datos estadísticos entregados.

Sobre la información estadística que se entrega, se hacen las siguientes aclaraciones:

a) Los datos estadísticos se entregan según registros de las Bases de Datos del Sistema de Información y Gestión Automatizada del Proceso Fiscal (SIGAP).
b) En general, los cuadros estadísticos contienen información únicamente de las categorías que se encontraron registros, de acuerdo a los criterios establecidos por el peticionario.
c) La información proporcionada respecto a casos ingresados y casos en investigación activa en sede administrativa o fiscal corresponden a casos iniciados en el período solicitado.
d) Los datos estadísticos respecto a *"Número de casos en que se presentó dictamen"*, corresponde a la cantidad de dictámenes elaborados por los delitos de la Ley Especial contra Delitos Informáticos y Conexos sucedidos en el departamento de San Miguel. Los cuales son independientes a la fecha de inicio de caso.

Notifíquese, al correo electrónico señalado por el solicitante, dando cumplimiento a lo establecido en los artículos 62 LAIP, 58 y 59 del Reglamento LAIP.

Licda. Deisi Marina Posada de Rodríguez Meza
Oficial de Información.