SISTEMATIZACIÓN DEL CURSO VIRTUAL

CIBERDELINCUENCIA

CURSO LA CIBERDELINCUENCIA: TRATAMIENTO PREVENTIVO, PROCESAL Y SUSTANTIVO DESDE UNA PERSPECTIVA INTERNACIONAL

Segunda edición

2021

Consejo General del Poder Judicial

Aula Iberoamericana
Consejo General del Poder Judicial

Cooperación Española
CONOCIMIENTO / INTERCOONECTA

CONTENIDO

INTRODUCCIÓN

Del 02 al 12 de noviembre 2021 el Centro de Formación de la Cooperación Española en Cartagena de Indias desarrolló la segunda versión del Curso virtual **"La Ciberdelincuencia: tratamiento preventivo, procesal y sustantivo desde una perspectiva internacional"**, un espacio de reflexión y debate, construido sobre el ambicioso objetivo de buscar una adecuada respuesta a los nuevos fenómenos delictivos que amenazan de manera global el tejido social de los diferentes países donde este esfuerzo académico espera lograr un eco a través de los profesionales del derecho a los que se dirigió esta actividad en países como Colombia, Argentina, Brasil, Perú, Chile, Nicaragua, Guatemala, El Salvador, Panamá, Uruguay, Paraguay, Cuba, República Dominicana, Costa Rica, Ecuador y Honduras.

En este espacio de formación se tuvo la oportunidad de compartir experiencias y discutir ideas desde diferentes puntos de vistas sobre las temáticas relacionadas con la normatividad, la dogmática y el tratamiento procesal en el contexto de la ciberdelincuencia. Todo lo anterior, bajo la coordinación de Alberto Varona Jiménez, Magistrado de la Audiencia Provincial de Barcelona y profesor de Derecho Penal y Procesal Penal de la Escuela Judicial de Consejo General del Poder Judicial de España; así mismo con la activa participación de Eloy Velasco Núñez, Magistrado de la Sala de Apelaciones de la Audiencia Nacional y Joaquín Delgado Martín, Magistrado de la Sala Penal de la Audiencia Nacional, quienes de manera magistral facilitaron la construcción de un marco conceptual que sirvió como referente para que los asistentes al evento abordaran el debate desde la particular perspectiva de sus diferentes países.

Sin lugar a dudas, la dinámica de trabajo empleada para el intercambio de saberes que hoy se recogen en este documento permitirá al lector reconocer la emergencia -en tiempos de globalización y de sociedades cada vez más soportadas en su cotidianidad por las tecnologías de la información- de comportamientos delictuales que afectan bienes jurídicos personalísimos como la intimidad, el secreto profesional, el patrimonio económico, la libertad, integridad y formación sexual, así como la afectación de un nuevo derecho fundamental que desarrolla la jurisprudencia del Tribunal Constitucional Español: el derecho fundamental a la Protección Eficaz del Entorno Virtual. El contexto de esta realidad está signado por un proceso de modernización extremo que desemboca en lo que algunos denominan Sociedad del Riesgo.

CIBERDELINCUENCIA ES HIJA DE SU TIEMPO

Los comportamientos que la comprenden trascienden el marco del Estado-Nación, como todos los fenómenos sociales en tiempos de globalización. En ese sentido, se hace imprescindible la discusión para adaptar -desde una perspectiva de Política Criminal- las legislaciones penales de cada país para hacer eficaz la persecución penal de las conductas que constituyen ciberdelincuencia en el marco de un derecho penal acorde con un estado social y democrático de derecho.

Este panorama tiene un grado de complejidad aguda, en la medida en que la Ciberdelincuencia es hija de su tiempo. Los comportamientos que la comprenden trascienden el marco del Estado-Nación, como todos los fenómenos sociales en tiempos de globalización. En ese sentido, se hace imprescindible la discusión para adaptar -desde una perspectiva de Política Criminal- las legislaciones penales de cada país para hacer eficaz la persecución penal de las conductas que constituyen ciberdelincuencia en el marco de un derecho penal acorde con un estado social y democrático de derecho.

En ese orden de ideas, en el marco de esta segunda edición del curso se logró llegar a heterogéneos hallazgos, conclusiones y recomendaciones que permitieron actualizar y realizar un seguimiento al estado del conocimiento y experiencias que circundan esta puntual temática en cada latitud, mismas que fueron recogidas en dos capítulos. En el primero describiremos el tratamiento que se le ha dado a la Ciberdelincuencia en el contexto internacional, teniendo en cuenta los desarrollos dogmáticos y procesales e identificando los aspectos problemáticos en la órbita de cada uno de ellos. En el segundo, se hará referencia a las conclusiones y recomendaciones que surgieron en el desarrollo de los foros temáticos y de discusión realizados en el curso.

Por último, no sobra agradecer de manera especial a todos aquellos participantes en este proyecto, que de manera directa o indirectamente han permitido nutrir la construcción de este producto de conocimiento al hacer accesible una temática por antonomasia compleja dada a la cantidad de factores técnicos y conocimientos especializados que se integran para su compresión, pero por sobre todo al dotarle de concreción, sensibilidad y pertinencia para la particular realidad judicial de cada latitud o territorio donde se abordó su estudio.

En suma, lo anterior constituye el valor agregado de este esfuerzo académico que busca acercarnos cada vez más a las perspectivas de aquellos fenómenos sociales tan vigentes en esta era pero que suelen pasar desapercibidos en el imaginario colectivo al ubicar la ciberdelincuencia como una realidad todavía lejana a nuestra cotidianidad y en consecuencia, relegando su atención y tratamiento a un plano oscuro y alejado del foco del interés público como si de un titán desterrado al Tártaro luego de la titanomaquia se tratara.

En ese sentido, cobran vigencia las palabras del filósofo español Ortega y Gasset cuando sentenció que *"solo es posible avanzar cuando se mira lejos, sólo cabe progresar cuando se piensa en grande".*

Cartagena de Indias
Del 02 al 12 de noviembre 2021

1

CIBERDELINCUENCIA

"Por 'ciberdelincuencia' se entiende cualquier forma de criminalidad ejecutada en el ámbito de interacción social definido por el uso de las Tecnologías de la Información y la Comunicación."

El paso de una sociedad industrial a una sociedad postindustrial ha traído como consecuencia un cambio cualitativo en todos los ámbitos de los entramados sociales. Lo anterior, obedece a una de las características de la sociedad postindustrial, como es el hecho de que el conocimiento científico se convierte en una fuerza productiva que modela y transforma las relaciones sociales, tal y como había existido hasta finales de la década del 50 del siglo XX, en las naciones hasta ese momento más altamente diferenciadas. Este cambio ha suscitado que, desde el punto de vista económico, la dimensión terciaria de la economía adquiera un protagonismo inusitado, convirtiéndose la venta de servicios, entretenimiento y comunicaciones, en los renglones más significativos de los países más desarrollados. Todo conocimiento que pueda ser traducido al lenguaje de la máquina, del ordenador, es un conocimiento que genera riqueza.

Seguidamente, con el desarrollo de las tecnologías de la información y la comunicación, así como de la Internet a finales del siglo XX, les imprimieron velocidad a estos cambios hasta el punto de que, todo lo que una persona común realiza de manera cotidiana, está mediado por dispositivos electrónicos y por las tecnologías de la información y la comunicación. Desde pagar las facturas de los servicios públicos domiciliarios, hasta concertar una cita amorosa. Todo está mediatizado por el lenguaje del Bit[1].

Estas transformaciones de las sociedades, donde la economía, el hogar, la escuela, la empresa y el Estado están conectados en tiempo real y relacionados por dispositivos electrónicos y tecnologías de la información y de la comunicación, permite que simultáneamente a estos cambios, surjan comportamientos delincuenciales producto de estas revoluciones. A estas nuevas manifestaciones criminales se les denomina: Ciberdelincuencia.

Hay que señalar que, en España, en su derecho interno, no se define qué es la Ciberdelincuencia. En su código penal, la Ley Orgánica 10 de 1995 en sus más de 24 títulos, en ningún capítulo se define que es la ciberdelincuencia. Obviamente, existen conductas que pueden comprenderse bajo el rotulo de ciberdelincuencia, pero su descripción se encuentra desperdigada por el todo el Código Penal Español, es diferentes títulos. Sin embargo, desde una perspectiva

[1]Unidad mínima de información.

internacional se encuentra una definición de ciberdelincuencia en el "Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia", del año 2014, en su artículo 2 numeral 1:

> *"Por 'ciberdelincuencia´ se entiende cualquier forma de criminalidad ejecutada en el ámbito de interacción social definido por el uso de las Tecnologías de la Información y la Comunicación."*

Es importante señalar que las Tecnologías de la Información y la Comunicación (TIC), son una combinación de medios informáticos con medios de comunicación y comprenden: sistemas informáticos, redes sociales, ordenadores, foros virtuales, etc. Las TIC han adquirido un desarrollo y han generado una necesidad abrumadora a partir de la entrada en vigor de la Internet en la década el siglo XX. Pues es en este contexto donde la ciberdelincuencia y el ciberdelito, considerados comportamientos criminales que se dan en el marco de las TIC, entran a desarrollarse en el ciberespacio, entendido como aquella realidad virtual en el que se agrupan páginas web, chats, usuarios y servicios de internet, a diferencia del delito informático, en el que se utilizan medios informáticos para su comisión, ya sea mediante un medio informático para consumar el punible o que el medio informático sea el objeto de la conducta criminal.

Este desarrollo intempestivo de las TIC forma parte de una evolución cuyo ritmo se aceleró a finales de la década del 50 del siglo XX. En el año de 1958 surge DARPA (Agencia de Proyectos de Investigación Avanzada de Defensa), adscrita al Ministerio de Defensa de los Estados Unidos con un uso exclusivamente militar. El objetivo de DARPA era conectar informáticamente las distintas agencias militares. En 1963 Joseph Carl Robnett Licklider, ingeniero informático, crea el concepto de Red de Computadoras, que va a cristalizar posteriormente en 1967 con el nacimiento de ARPANET, el origen y antecedente de la Internet. El proyecto de ARPANET consistía en conectar diferentes computadoras pertenecientes a prestigiosas universidades de vanguardia en la investigación en tecnologías de la información, así como a varios institutos en el mismo ramo: MIT, RAND CORPOTATION, IML. En 1969 se dio la primera conexión o red de computadoras entre las universidades de UCLA y Stanford. Y en 1972 se envía el primero correo electrónico. A finales de la década de los ochenta del siglo XX, se va a dar otra transformación importante que abonará el camino para el uso global y cotidiano de la Internet: el cambio de protocolo de información NCP a TCP/IP.

Estas transformaciones sociales productos del avance de las tecnologías de la información y la comunicación generan, en simultánea, comportamientos ciberdelincuenciales con las siguientes características: ↓↓↓

Anonimato: delitos cometidos a distancia, sin posible reacción inmediata de la víctima.

Rapidez: delitos de comisión instantánea.

Delitos masa: afectación a un número indeterminado de personas.

Autores: los menores de edad puede ser fácilmente sujetos activos de la conducta.

Facilidad de medios: estos delitos pueden ser realizados desde ordenadores, celulares y otros dispositivos electrónicos.

Componente internacional: en la comisión de este tipo de delitos no hay fronteras. Trasciende el marco del Estado Nación.

Desde la perspectiva internacional, teniendo en cuenta los instrumentos y particulares instituciones de cooperación internacional, es importante destacar a la Conferencia de Ministros de Justicia de los Países Iberoamericanos (COMJIB), así como también del Consejo de Europa creado por el Tratado de Londres de 1949. En el marco del Consejo de Europa, surge en el año 2001 el Convenio del Consejo de Europa para la Ciberdelincuencia de Budapest. Posteriormente, en el 2003 surge el protocolo adicional al convenio sobre la Ciberdelincuencia, concerniente a la penalización de actos de índole racial y xenófobo cometido por medios informáticos, firmado en Estrasburgo, el 28 de enero 2003. El Convenio de Budapest es de suma importancia, ya que es el primer tratado internacional que busca establecer principios y bases normativas para perseguir penalmente a la ciberdelincuencia teniendo como horizonte unos criterios fundamentales:

Finalmente, en el marco de los esfuerzos y compromisos suscritos por los estados frente a la adecuada respuesta al fenómeno de la cibercriminalidad en el plano internacional resulta necesario destacar que el convenio de Budapest ha sido ratificado por 65 países, además de multitud de Estados de Europa y de otras regiones (Estados Unidos, Canadá, Japón, Australia, Marruecos…) y por países del ámbito iberoamericano (Costa Rica, Colombia, Perú, Paraguay, República Dominicana, Argentina, Chile, Panamá, Portugal y España). En el ámbito de la COMJIB, existe el *"Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia"* del 28 de mayo del 2014. Junto a esta normativa, como directriz interpretativa, está la recomendación del COMJIB relativa a la tipificación y sanción de la ciberdelincuencia del 28 mayo del 2014 realizada en Madrid. En Latinoamérica, los países que han firmado el convenio son: Guatemala, Cuba, México, Perú, Nicaragua, Uruguay y Costa Rica.

1.1 Tratamiento sustantivo

Durante este espacio se abordó el estudio dogmático de los comportamientos que configuran ciberdelitos. Por esta razón resulta pertinente destacar en la mente del lector una premisa elemental para la caracterización de estos comportamientos; esto es que, desde un enfoque criminológico, la cibercriminalidad constituye una especial faceta delictiva de cuello blanco tal como lo destaca la profesora Alastuey Dobon[2], y que dado al especial contexto histórico en el que se concibe su configuración es un fenómeno social que se integra dentro de la agenda política criminal del nuevo derecho penal.

Lo anterior, claramente impone como consecuencia la necesidad de replantear la visión tradicional con la que se aborda el fenómeno criminal, pues ante la irrupción de nuevos comportamientos a todas luces antijuridicas, las legislaciones penales atadas a las viejas formulas de la criminalidad común pueden verse rezagadas hasta el punto de propiciar la impunidad.

Un claro ejemplo de lo anterior fue la legislación penal colombiana antes de la expedición de la Ley 1273 de 2009 por medio del cual se modificó el Código Penal vigente y se introdujo como interés jurídico objeto de tutela penal, la protección de la información y los datos. En aquel interregno caracterizado por un conocimiento fragmentado del cibercrimen el ordenamiento jurídico colombiano fue considerado un verdadero paraíso informático al permitir la impunidad estructural en este material tal como lo destaca el profesor Posada Maya[3]. Situación esta última, común a varios países en el plano latinoamericano como Bolivia, Uruguay o Argentina, donde no existe una tipificación sistematizada bajo un mismo titulo para los delitos informáticos. Aunque para el caso argentino puntualmente solo a partir de 2008 se sancionó la Ley 26.388 para delitos informáticos adoptándolos parcialmente en su legislación, a pesar de su adhesión al convenio sobre cibercriminalidad de Budapest en el año 2001.

De allí la importancia de elaborar e interiorizar nuevos planteamientos de orden dogmático y de cohorte político criminal tendientes a volver más eficiente la cooperación entre estados en el plano internacional, así como auspiciar la adecuada respuesta en el plano nacional a través de la configuración de herramientas conceptuales que sean respetuosas de los postulados consti-

[2]Consúltese entre otros: Apuntes sobre la perspectiva criminológica de la delincuencia informática patrimonial.

[3]Consúltese entre otros: Los cibercrímenes: Un Nuevo paradigma de criminalidad. Universidad de los Andes. Editorial Ibáñez. Pág. 34

1.1.1 Ciberdelincuencia económica

> **se caracteriza fundamentalmente porque el delincuente, mediante el uso de dispositivos y tecnologías informáticas, se apodera de dineros y activos ajenos para su beneficio lucrativo o de un tercero**

En el plano de la caracterización de las diferentes géneros de conductas delictivas asociadas al contexto del cibercrimen resulta útil plantear como herramienta metodológica la identificación de un bien o interés jurídico susceptible de tutela penal a partir del cual se esbocen los diferentes presupuestos normativos de orden objetivo y subjetivo de cada tipo de modalidad conductual.

En ese orden de ideas, desde la óptica constitucional para la identificación de un bien jurídico podremos destacar el carácter compuesto o pluriofensivo de aquellas conductas que se configuren bajo la etiqueta de ciberdelincuencia económica, por cuanto es fácil intuir que la misma se caracteriza fundamentalmente porque el delincuente, mediante el uso de dispositivos y tecnologías informáticas, se apodera de dineros y activos ajenos para su beneficio lucrativo o de un tercero, es decir, converge un atentado al patrimonio económico del sujeto pasivo como interés individual al tiempo de una afectación al derecho fundamental de "*la protección eficaz del entorno virtual*" como lo denomina la jurisprudencia del Tribunal Constitucional Español; similar a la denominación entregados en otros escenarios como el relativo a *"la protección de la información y de los datos"* en el plano colombiano, o el que gira en torno a los delitos contra "*los datos y sistemas informáticos"* en Perú.

1.1.1.1 Tipología

Partiendo de las anteriores consideraciones generales es posible destacar como formas típicas de la ciberdelincuencia económicas los siguientes modelos conductuales:

Para el caso del Código Penal Español[4] , trae una serie de tipos penales que se encuentran en diferentes títulos del cuerpo normativo pero que se consideran por antonomasia ciberdelincuencia económica. Un ejemplo de ello es el Tipo Penal de Estafa establecido en el artículo 248 del Código Penal de España- Ley Orgánica 10/1995 – que sobre el particular señala bajo el capitulo VI sobre "las defraudaciones" lo siguiente:

[4]Ley Orgánica 10/1993, del 23 de noviembre.

Artículo 248.

1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

45% de los escritos de acusación del Ministerio Fiscal son estafas informáticas

De cara a la realidad española se conoce que el 45% de los escritos de acusación del Ministerio Fiscal son estafas informáticas. En ésta última, el delincuente o el hacker engaña a través de medios informáticos. La estafa como modalidad delictiva tiene dos formas: la sociológica y la mecánica o maquinal.

En la modalidad sociológica de la estafa se hace necesario todo un despliegue del engaño contando con la presencia del autor o autores y su relación con las víctimas en el contexto de las TIC. Su preparación, ejecución y consumación se hace por medios informáticos. Como ejemplo podemos citar: las cartas nigerianas[5], el phishing[6], las falsas cartas de los departamentos de hacienda.

Por otro lado, la estafa maquinal consiste en la utilización de artificios técnicos que recaen en la maquinas (cajeros automáticos) con el objetivo de apoderase fraudulentamente de los dineros. En la actualidad se asume que el pharming es una forma de estafa maquinal, pues en esta se manipula el Servidor del Número de Dominio (DNS) para obtener claves e información de las víctimas enviándolas a páginas web distinta a la que quiere acceder el usuario.

En tono con lo anterior, la legislación penal española asume como punible el simple acto preparatorio de poseer, fabricar o vender software para estafar. En otras palabras, incurre en estafa la persona que posea un software que sólo sirva para estafar pues desde una perspectiva político criminal, el tipificar tipos penales de peligro abstracto contribuyen a regular la cibercriminalidad económica. La legislación penal española también ha tipificado como modalidad de estafa, la utilización de los datos contenidos en las tarjetas bancarias de manera fraudulenta, en perjuicio del titular de esta o de terceros. Esto sucede cuando el titular de la tarjeta bancaria la utiliza para pagar bienes o servicios, el delincuente "*clona*" la información que tiene la tarjeta, esto es, los algoritmos que establecen quien es propietario de la tarjeta, las cuentas y los activos que hay en ellas y posteriormente se hace pasar por el titular de la tarjeta para apropiarse de los dineros.

[5] Un fraude informático consistente en ilusionar al incauto con una gran suma de dinero, pero persuadiéndolo en que la condición para acceder a ella, es pagando una suma de dinero por adelantado.

[6] Estafa que consiste en obtener información confidencial de formar fraudulenta como cuentas y códigos bancarios.

Desde una perspectiva de derecho comparado surge como un hecho corroborable a través de las experiencias compartidas por todos los participantes, que el abordaje del delito de estafa por medios informáticos es posible gracias a la implementación de figuras típicas autónomas, que reprochan de manera concreta la conducta causante del perjuicio económico como en el caso colombiano a través del artículo 269J de la Ley 599 del 2000 con el punible de transferencia no consentida de activos, cuyo diseño se recoge los presupuestos descritos en los literales A y B del numeral 2 del artículo 248 de la ley española, dictando lo siguiente:

> **ARTÍCULO 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.** El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

En igual sentido, la legislación argentina contempla en el título VI, capítulo IV de su Código Penal – Ley 11.179- en lo relativo al delito de estafa el artículo 173, numeral 16, incorporado por la Ley No. 26.388 del 2008, establece que una de las formas de tipicidad de a conducta se da cuando:

> **16.** El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

Así mismo, el artículo 363Bis del Código Penal Boliviano contempla dentro de su capítulo XI sobre delitos informáticos el relativo a la "manipulación informática", mediante el cual se pune la conducta que causa perjuicio económico empleando medios informáticos en los siguientes términos:

ARTICULO 363 bis. - (MANIPULACIÓN INFORMÁTICA). - El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

En ese mismo sentido, bajo la fórmula de contemplar un delito autónomo que recoge el perjuicio económico que se realiza a través de medios informáticos se aprecian las legislaciones ecuatorianas (Árt, 186 inciso 1 y 2) Costa Rica (Árt. 217bis) entre otras.

No obstante todo lo anterior, en el caso de países que no tipifican de manera taxativa alguna forma de obtener lucro económico en perjuicio de un tercero valiéndose de medios informáticos, tales como Brasil, Uruguay y Honduras, entre otros, se acude a la fórmula consagrada con antelación en sus códigos penales, estos son las

Aplica también como ciberdelincuencia económica los

...delitos contra la propiedad intelectual |

según el artículo 270 del Código Penal español. O cuando haya plagio, distribución fraudulenta de una obra, conocimiento científico, literario, industrial y artístico a través de las nuevas tecnologías, sin la autorización de sus titulares.

descripciones previstas para los delitos de hurtos o estafas, buscando encuadrar típicamente los contornos de cada manifestación delictiva dentro de los modelos conductuales básicos, que contempla cada hipótesis delictiva en aras de superar la ausencia de legislación especial para el caso concreto.

Otro ejemplo de ciberdelincuencia económica lo constituye la defraudación, artículo 255 del Código Penal de España. Este comportamiento criminal se caracteriza, en que mientras unas personas sufragan un servicio: agua, luz, internet; de manera arbitraria, otro goza y usufructúa el servicio sin que su legítimo titular lo haya consentido o autorizado. En materia de telecomunicación la defraudación puede hacerse valiéndose de los siguientes medios: (i) instalando mecanismos para realizar la defraudación y (ii) alterando los aparatos contadores.

Dentro de los ciberdelitos económicos encontramos también el hurto de tiempo, artículo 256 del Código Penal español. Esta conducta consiste en utilizar terminales telecomunicacionales ajenos, en contra del fin para el que están establecidos, generando un perjuicio económico.

También se tipifica en la legislación española el delito de daño informático y denegación de servicio, artículo 264 del Código Penal español, el cual tiene dos modalidades: (i) se penaliza a quien por cualquier medio y sin autorización borre, dañe, deteriore, altere, suprima o haga inaccesible datos informáticos, programas informáticos o documentos informáticos ajenos, lo que se denomina cracking[7]; (ii) también se penaliza a quien interrumpa u obstaculice el sistema informático ajeno sin estar autorizado para ello, conocido como *denial of service*[8]. Este delito se agrava si la conducta se comete en el marco de una organización criminal, si el daño causado es de especial gravedad o ha afectado un gran número de sistemas informáticos, si la conducta afecta el funcionamiento de servicios públicos o afecta la provisión de bienes considerados de primera necesidad. Por otro lado, el artículo 264 del Código Penal español castiga con pena de prisión a la que persona que, sin estar debidamente autorizada, produzca, adquiera para su uso, importe o facilite a terceros: (i) un programa informático para cometer daño informático o denegación de servicio informático; (ii) contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Aplica también como ciberdelincuencia económica los delitos contra la propiedad intelectual e industrial según el artículo 270 del Código Penal español. O cuando haya plagio, distribución fraudulenta de una obra, conocimiento científico, literario, industrial y artístico a través de las nuevas tecnologías, sin la autorización de sus titulares. El mencionado artículo señala que será penalizada la persona o personas que "con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente, en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios". Este atentado contra la propiedad intelectual e industrial puede realizarse también bajo otras

[7] Acceso ilícito y dañoso a un sistema informático.

[8] Ataque un sistema de computadores o a una Red, que ocasione que sus titulares legítimos no puedan acceder a ella.

modalidades. Una de ellas consiste en los llamados delitos de referenciación, en los cuales el hacker indica a los usuarios informáticos los enlaces, productos y lugares en los cuales pueden disfrutar, acceder y sin autorización del titular o inventor de la obra literaria, científica, etc., de manera gratuita, esto es, sin remuneración alguna. Otra modalidad consiste en que el hacker o el delincuente facilita los medios para eludir las medias de protección tecnológica que protege la propiedad intelectual frente a terceros.

La legislación española en su artículo 284 del Código Penal describe el delito de "alteración de precio de las cosas", en el que se penaliza a la persona o personas que de "manera directa o indirecta o a través de un medio de comunicación, por medio de internet o mediante el uso de tecnologías de la información y la comunicación, o por cualquier otro medio, difundieren noticias o rumores o transmitieren señales falsas o engañosas sobre personas o empresas, ofreciendo a sabiendas datos económicos total o parcialmente falsos con el fin de alterar o preservar el precio de cotización de un instrumento financiero o un contrato de contado sobre materias primas relacionado o de manipular el cálculo de un índice de referencia, cuando obtuvieran, para sí o para tercero, un beneficio".

1.1.2 Ciberdelincuencia intrusiva

> **...bien o interés jurídico susceptible de tutela penal los relacionados con datos o información sensible de la vida íntima**

Siguiendo la metodología empleada en el capítulo inmediatamente anterior, para la caracterización preliminar de este bloque de delitos basta con identificar como bien o interés jurídico susceptible de tutela penal los relacionados con datos o información sensible de la vida íntima de una persona relacionada comúnmente con la órbita sexual del afectado y empleando para su fin las TIC.

1.1.2.1 Tipología

Son ejemplos clásicos de esta forma de conductas los relacionados con la pornografía infantil, articulo 189 Código Penal español, el abuso sexual, artículo 183 bis, el llamado *Child Grooming*, artículo 183 ter del Código Penal, así como el descubrimiento y revelación de secretos, artículo 197 del Código Penal.

23% **de los escritos de acusación versan sobre el delito de pornografía infantil como delito informático**

En España, el 23% de los escritos de acusación versan sobre el delito de pornografía infantil como delito informático. Este tipo penal busca amparar el bien jurídico del crecimiento armónico de la sexualidad del menor. Que el menor en el desarrollo de su integridad y formación sexual no tenga ninguna interferencia que pueda afectar su normal desarrollo.

Según la Directiva 2011/93/UE, la pornografía infantil es la participación del menor o persona con discapacidad en una conducta sexual explícita –real o simulada-, o la representación de sus órganos sexuales con un fin principalmente sexual –excluyendo el arte o el mero erotismo tolerado por las convenciones sociales, por ejemplo-, o la representación que parezca lo anterior, real o simulado, salvo que el representado al momento de su realización sea mayor de 18 años, y las imágenes realistas de la participación del menor o persona con discapacidad en una conducta sexualmente explícita o de sus órganos sexuales con fin principalmente sexual.

En lo que respecta a su configuración típica este delito se exige que exista un menor de 18 años y la existencia de actos o imágenes que tenga un marcado contenido sexual. La conducta se agrava cuando el menor es de 16 años, se cosifica a la víctima mediante actos degradantes, cuando se utiliza la violencia, tener un deber de cuidado y custodia sobre la víctima. Muy unido a este tipo penal se encuentran las conductas que son perseguidas

penalmente, pero sus sanciones son menores: asistir a espectáculos de pornografía infantil, adquirir o poseer pornografía infantil para uso propio, acceder a pornografía infantil mediante las TIC. En material procesal, desde la etapa de investigación el juez puede ordenar como medida cautelar bloquear o retirar el acceso a páginas web y/o aplicaciones que contengan o difundan pornografía infantil.

Como ciberdelitos intrusivos que afectan la libertad y formación sexual encontramos el artículo 183 bis del Código Penal español, que tipifica el tipo penal de abuso sexual. Incurre en este tipo aquel que, con fines sexuales, determine a un menor de 16 años a participar en un comportamiento de naturaleza sexual, o le haga presenciar actos de carácter sexual, aunque el autor no participe en ellos. También es sujeto activo de esta conducta la persona que, sin haber participado, le haga presenciar abusos sexuales al menor de edad. Otro ciberdelito intrusivo bastante común en estos tiempos es el que la doctrina denomina el *child grooming*, el cual se encuentra tipificado en el artículo 183 ter del Código Penal español. Esta conducta opera en dos dimensiones:

- Contactar a un menor de 16 años a través de cualquier tecnología de información y la comunicación, para gestar un encuentro con la finalidad de realizar un delito abuso sexual o de pornografía infantil. También propiciar el encuentro para realizar actos materiales de acercamiento.

- El que, a través de cualquier tecnología de la información y comunicación, internet o teléfono, se comunique con un menor con la finalidad de embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor.

Otro ciberdelito intrusivo es el acoso, que se encuentra regulado en el artículo 172 ter del Código Penal español. Para que esta conducta se configure se necesitan dos condiciones: (i) que el agobio y el hostigamiento que el autor realiza sobre la víctima sea insistente y reiterado, y (ii) en virtud de ello, se altere de manera grave el desarrollo de la vida cotidiana de la víctima. En ese sentido, el mencionado artículo señala las siguientes conductas constitutivas de acoso sobre una persona:

a) La vigile, la persiga o busque su cercanía física.

b) Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.

c) Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.

d) Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.

EL DELITO DE ACOSO

El delito de acoso se agrava si la conducta recae sobre personas que estén una situación especial de vulnerabilidad, ya sea por razones de enfermedad, raza, género, etc.

El delito de acoso se agrava si la conducta recae sobre personas que estén una situación especial de vulnerabilidad, ya sea por razones de enfermedad, raza, género, etc. Por otra parte, la investigación por esta conducta sólo puede adelantarse si el propio agraviado o agraviada, interpone la denuncia por sí mismo o a través de apoderado. También la legislación penal española trae como delito ciberintrusivo el quebrantamiento del alejamiento, consagrado en el artículo 468 numeral 3 del Código Penal español. Ante este tipo de conductas, un juez impone un distanciamiento entre el autor y la víctima y señala que estos tienen que mantener determinada distancia o no frecuentar particulares lugares, estableciendo como control el uso de pulseras o dispositivos telemáticos que controlan la geolocalización para verificar si se está respetando o incumpliendo el alejamiento. Se incurre en la conducta mencionada aquella persona que -estando obligada judicialmente a llevar la pulsera y guardar el alejamiento-, inutilice y perturbe el funcionamiento de los dispositivos telemáticos de geolocalización, no los lleve consigo u omita las medidas para mantener el óptimo funcionamiento del artefacto.

Otro ejemplo, bastante característico de lo que es la ciberdelincuencia intrusiva, es el descubrimiento y la revelación de secretos *(Hacking)*, consagrado en el artículo 197 del Código Penal español. Esta conducta es el ciberdelito por antonomasia, ya que el autor o los autores -mediante el uso de software malicioso: *Troyano*[9], *Spyware*[10], *Keyloggers*[11], *Botnest*[12], *virus*[13] - busca descubrir los secretos o vulnerar la intimidad de una persona, se apodera de sus papeles, cartas, mensajes de correo electrónico o cualquiera otro documento o efectos personales, intercepta sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación. El artículo 197 bis, en relación con esta conducta, señala que será castigada la persona que, por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo. Así será castigado la persona o personas que, a través de la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos.

Es necesario mencionar que, en el curso sobre ciberdelincuencia se hizo alusión a la utilización de las TIC, como instrumentos para perpetrar delitos considerados tradicionales en materia

[9] Malware (Software malicioso) que se presente al usuario como legítimo, pero que, al ser utilizado por el usuario, le permite al hacker o al delincuente un acceso desde la distancia, al equipo infectado.

[10] Es un Malware que consiste en espiar los dispositivos electrónicos que una persona utiliza con el fin de saber sus hábitos, sin su autorización, para recopilar esta información para el uso del hacker o el delincuente.

[11] Este es un software y también puede ser un dispositivo Hardware que se utiliza para registrar las pulsaciones que se realizan sobre el teclado, para interceptar la información sin que el usuario lo note.

[12] Hace referencia a un conjunto de computadores infectados que de forma remota pueden ser utilizados por el hacker o el delincuente para realizar ataques informáticos.

[13] El virus informático es un software que busca alterar el normal funcionamiento de un dispositivo informático -sin la autorización del legitimo usuario del dispositivo-, con fines espurios.

penal, como son la injuria y la calumnia, tipificados en los artículos 205 y 208 del Código Penal español. En ese sentido, se configuran estás conductas cuando a través de blogs, redes sociales, correo electrónico etc, una persona realiza imputaciones deshonrosas a otra o le atribuya conductas punibles: hurto, homicidio, acceso carnal, etc. La legislación española exige -para respetar el derecho fundamental a la Libertad de Expresión- que los insultos y calumnias deben ser los más graves, teniendo en cuenta el contexto social, para que se puedan tipificar.

En la misma línea de delitos tradicionales, cometidos por medio de las nuevas tecnologías de la información y la comunicación, la legislación española tipifica las amenazas leves artículo 171.7 del Código Penal y las coacciones leves, artículo 172.3. En ese sentido, también se incurre en estas conductas cuando una persona, a través de las TIC, ataca el sosiego y la tranquilidad de otras personas, mediante coacciones u amenazas que afectan el desarrollo normal de la vida cotidiana de la víctima y su libertad de obrar modificando su comportamiento. Dentro de los delitos tradicionales también existe -que pueden ser cometidos instrumentalizando las nuevas tecnologías-, la conducta punible de: extorsión, artículo 243 del Código Penal español.

Por medio de las TIC se vienen presentando situaciones en las que, a los usuarios informáticos, se les bloquean accesos o se las roban informaciones de sus sistemas informáticos y sólo mediante un pago pueden recuperar los accesos o la información. También personas que, conociendo los enlaces y contactos sexuales de un usuario, se hacen pasar por policías -*ransomware*[14] - en sus mensajes extorsionadores y le exigen un pago en dinero -al usuario- para no denunciarlo o exponerlo.

Por otro lado, el Código Penal español en sus artículos 417 -423 consagra el delito de infidelidad en la custodia de documentos o la violación de secretos públicos para su propia venta. Es una conducta que sólo puede cometer el funcionario público y se consuma cuando este cede o divulga datos que conoce por su profesión, los cuales tienen que estar en reserva. De reciente tipificación en la legislación penal ibérica es el delito de: contra el orden público, establecido en los preceptos legales, artículos 559-560 del código penal. Se materializa esta conducta cuando -en las situaciones que, con ocasión de protestas, manifestaciones y alteraciones del orden público, en las cuales se destruyan bienes públicos o privados-, a través de las nuevas tecnologías, se incite, se difundan o se distribuyan mensajes y consignas públicamente que muevan a las personas a cometer conductas agravadas contra el orden público o refuercen la decisión de perpetrarlos. Las conductas agravadas que alteran el orden público son las siguientes:

1. Los daños que interrumpan, obstaculicen o destruyan líneas o instalaciones de telecomunicaciones o la correspondencia postal.

2. Los daños en vías férreas que originen un grave daño para la circulación ferroviaria.

3. Los daños contra las conducciones o transmisiones de agua, gas o electricidad para las poblaciones, interrumpiendo o alterando gravemente el suministro o servicio.

[14] Es un software malicioso que infecta computadores, smartphone y muestran mensajes que exigen el pago del dinero para restablecer el funcionamiento del sistema.

Finalmente, en el Curso sobre Ciberdelincuencia, como modalidad de delito ciberintrusivo, se estudió el delito de incitación al odio y a la violencia contra grupos/diferentes, establecido en el artículo 510 del código penal, el cual puede realizarse a través de las nuevas tecnologías de la información y de la comunicación. Hay que señalar que este tipo penal no busca tipificar las manifestaciones de odio que hacen parte de los pensamientos, ideas o convicciones de las personas, ya sea por su visión de mundo, religión, concepción filosófica o política, toda vez que el odio como el amor son pulsiones humanas. En ese sentido, sólo se incurre en el presente delito cuando se realizan los siguientes comportamientos:

1. Fomentar, promover o incitar directa o indirectamente al odio, hostilidad, discriminación o violencia contra un grupo, una parte del mismo o contra una persona determinada por razón de su pertenencia a aquel, por motivos racistas, antisemitas u otros referentes a la ideología, religión o creencias, situación familiar, la pertenencia de sus miembros a una etnia, raza o nación, su origen nacional, su sexo, orientación o identidad sexual, por razones de género, enfermedad o discapacidad.

2. Facilitar a terceras personas el acceso, distribuir, difundir o vender escritos o cualquier otra clase de material o soportes que por su contenido sean idóneos para fomentar, promover, o incitar directa o indirectamente al odio, hostilidad, discriminación o violencia contra un grupo, una parte del mismo, o contra una persona determinada por razón de su pertenencia a aquel, por motivos racistas, antisemitas u otros referentes a la ideología, religión o creencias, situación familiar, la pertenencia de sus miembros a una etnia, raza o nación, su origen nacional, su sexo, orientación o identidad sexual, por razones de género, enfermedad o discapacidad.

3. Negar, trivializar gravemente o enaltecer los delitos de genocidio, de lesa humanidad o contra las personas y bienes protegidos en caso de conflicto armado, o enaltecer a sus autores cuando se hubieren cometido contra un grupo o una parte del mismo, o contra una persona determinada por razón de su pertenencia al mismo, por motivos racistas, antisemitas u otros referentes a la ideología, religión o creencias, la situación familiar o la pertenencia de sus miembros a una etnia, raza o nación, su origen nacional, su sexo, orientación o identidad sexual, por razones de género, enfermedad o discapacidad, cuando de este modo se promueva o favorezca un clima de violencia, hostilidad, odio o discriminación contra los mismos.

Las anteriores conductas se agravan cuando se realizan por los medios de comunicación social, por las tecnologías de la información y el internet, de tal manera que al mensaje de odio accedan un elevado número de personas.

Continuando con esta misma línea temática es posible destacar en el plano latinoamericano que la legislación penal colombiana a través de su título VII Bis contempla un capítulo especial destinado a este tipo de atentados contra información sensible de terceros. Concretamente en su capítulo primero se refiere a este grupo de conductas bajo el rótulo de atentados contra la confiabilidad, la integridad y la disponibilidad de datos y de los sistemas de información.

De allí se contempla un catálogo de delitos autónomos como lo son puntualmente:

- **Artículo 269a. Acceso abusivo a un sistema informático.**
- **Artículo 269c. Interceptación de datos informáticos.**
- **Artículo 269e. Uso de software malicioso.**
- **Artículo 269f. Violación de datos personales.**
- **Artículo 269g. Suplantación de sitios web para capturar datos personales.**

Todas estas figuras guardan correspondencia con los rasgos generales descritos con antelación al tomar como referencia la legislación española, con la excepción de que dentro de sus presupuestos normativos no se contempla de manera especifica el componente de orden sexual o abusivo como el que se relaciona con las modalidades del *child grooming*.

En igual sentido, pero con un alcance mayor en razón a la especialidad de figuras típicas, la legislación penal mexicana contempla dentro de su ordenamiento hipótesis delictivas destinadas a la protección de datos personas en posesión de particulares destinado dentro de la ley federal para ese aspecto el capítulo XI, destinado a los delitos en materia de tratamiento indebido de datos personales; los relativos al acceso ilícito a sistemas y equipos de informática.

1.1.3 Ciberespionaje y terrorismo

1.1.3.1 Tipología

Finalmente, otra conducta ciberdelictiva es el de espionaje informático de secretos de empresa. Los secretos de empresa son datos e informaciones propias de una actividad empresarial que si fueran conocidas por la competencia afectarían significativamente su capacidad competitiva. El acceso de forma fraudulenta a técnicas de producción, fórmulas de productos o lista de clientes de empresas o de empresas, con miras a afectar la competitividad de éstas configura espionaje informático. Asimismo, es importante señalar que, frente a conductas delictivas clásicas con repercusión económica y patrimonial, la legislación española consagra que estas también se consuman cuando son realizadas por medios informáticos o electrónicos, como el delito de falsedad según artículos 390-399, falsedad en documentos electrónicos.

También está el delito de falsedad de tarjetas, del artículo 399 bis del Código Penal, consistente en fabricar, en troquelar sobre los plásticos -(tarjetas)- datos y después utilizarlas en entidades bancarias o en el comercio. Y, por último, nos encontramos con el lavado de activos, consistente en introducir dineros provenientes de conductas delincuenciales - (estafa, tráfico de drogas, cohecho, etc.)- e introducirlos en mercados lícitos para bloquearlos y darles naturaleza de legitimidad. En este orden de ideas, con las tecnologías de la información y la comunicación se hace más fácil y rápida enviar dineros de procedencia criminal a paraísos fiscales o movilizarlos de tal forma que estos adquieran apariencia de legalidad.

1.2 Tratamiento procesal

"...toda sociedad democrática la manera como se regula su legislación procesal penal es una consecuencia profunda de las inquietudes humanas que acompañan su cotidianidad..."

De acuerdo por el autor argentino Julio Maier, *"el proceso penal es derecho constitucional reglamentado o reformulado"*, en la medida que la legislación procesal penal vigente en cualquier momento histórico es el reflejo de un compromiso asumido democráticamente por la sociedad consigo mismos para otorgar al Estado de un número concreto de mecanismos de persecución del delito, a cambio de ver limitados sus derechos fundamentales en procura de salvaguardar el resto de sus libertades.

De lo anterior, se extrae que en toda sociedad democrática la manera como se regula su legislación procesal penal es una consecuencia profunda de las inquietudes humanas que acompañan su cotidianidad, las cuales se mantienen en constante evolución para otorgar respuestas oportunas y pertinentes a cada malestar que pretenda colocar en riesgo su estabilidad y cohesión social.

En ese orden de ideas resulta pertinente señalar la necesidad y urgencia de las diferentes legislaciones en torno a la actualización y adecuación de sus herramientas conceptuales e investigativas con miras a responder de manera oportuna e idónea dentro de la actual discusión que se desprende de la persecución contra esta nueva forma de criminalidad.

1.2.1 Aspectos procedimentales sobre la persecución de la ciberdelincuencia

1.2.1.1- Límites constitucionales para la adquisición de fuente probatoria en el contexto de la ciberdelincuencia

En lo referente a los aspectos investigativos y procesales que regulan la persecución penal de los comportamientos que tienen la naturaleza de ciberdelitos, se hizo énfasis en los límites constitucionales y legales que limitan la potestad del Estado en el ejercicio de su poder punitivo.

Toda investigación que utilice medios tecnológicos como interceptaciones telefónicas, interceptaciones de telecomunicaciones como *whatsapp*, correo electrónico, SMS, así como la utilización de micrófonos ambientes o cámaras ocultas para capturar sonidos o imágenes de la personas o personas, la cesión de datos tele-comunicativos o los registros de almacenamiento de información, registros remoto de dispositivos y ordenadores, el agente encubierto o las utilización de dispositivos de geolocalización, resultan ostensiblemente invasivas de la esfera privada e íntima de las personas, lo que puede desembocar en una amenaza y vulneración de derechos y garantías fundamentales.

En España, con miras a conjurar estas situaciones, la Ley de Enjuiciamiento Criminal (reforma operada por la Ley Orgánica 13/2015) consagra que sólo el Juez de Instrucción es el único que puede decretar estas medidas de investigación con medios tecnológicos -sin perjuicio de que algunas de ellas puedan ser realizadas por la Policía en determinadas situaciones de urgencia y sometidas a la ratificación judicial-, y en la motivación de la decisión que decreta la medidas, debe estudiar si están debidamente acreditados los principios fundamentales de: autorización judicial[15], legalidad[16], especialidad[17],

[15] Solamente es el Juez el único por mandato de la constitución, que puede decretar mediante una decisión motivada por solicitud del Ministerio Fiscal, la autorización o no una medida de investigación con medios tecnológicos.

[16] Cualquier medida de investigación tecnológica para poder ser decretada por el juez debe estar prevista en un precepto legal. Sino está prevista, el juez no puede decretar la medida. Por otra parte, no basta con que este contemplada en el precepto legal, sino que esta medida debe ser conducente.

[17] Exige que el juez solo puede decretar investigaciones con medios tecnológicos cuando existe una investigación por la presunta comisión de un delito en concreto. No puede decretar medidas en abstracto, de tal forma que no podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva.

necesidad-excepcionalidad[18], idoneidad[19] y de proporcionalidad[20] . Y también radica en el juez, el control posterior de las medidas investigativas que autorizó, en las cuales se utilicen medios tecnológicos de investigación como los mencionados anteriormente. Por otra parte, como son tan invasivas estás medidas de investigación, están limitadas en el tiempo.

Se exige que quien solicita al juez la autorización de una medida de investigación tecnológica debe realizar unas determinadas cargas argumentativas: (i) debe describirle al juez el hecho investigado -(con sus características de conducta punible y sus circunstancias de modo, tiempo y lugar)-, el hecho concreto por el cual va a solicitar la medida para cumplir el principio de especialidad; (ii) debe justificar por qué en el caso concreto la medida de investigación tecnológica se hace necesaria, por qué con las otras menos invasivas no puede lograrse la finalidad probatoria; (iii) dependiendo el caso debe señalar cuales son las comunicaciones o dispositivos de las personas sobre las cuales va a recaer la medida de investigación tecnológica; (iv) el funcionario de policía judicial que va a tener a cargo y la manera en que se va a ejecutar la medida; (v) el tiempo de duración y (vi) el sujeto tecnológico obligado, la operadora o el experto tecnológico a través del cual se va a ejecutar esta media tecnológica de investigación.

Relacionado con lo anterior, la decisión del juez que resuelva esta solicitud debe ser debidamente fundamentada y motivada (auto o resolución), teniendo como horizonte que en un Estado social y democrático de derecho, la regla general es que ninguna persona puede estar contantemente vigilada e interceptada por organismos del Estado y solo podrá decretarse la autorización de investigación mediante medio tecnológico, por autoridad judicial una vez que la solicitud cumpla con los requisitos de legalidad, proporcionalidad, idoneidad, necesidad, especialidad, etc.

[18] Este principio le exige el juez analizar si existen otras medidas menos invasivas de los derechos fundamentales mediante las cuales se obtengan la misma finalidad probatoria. Porque si llegasen a existir otras medidas menos invasivas de los derechos fundamentales, la medida solicitada no es necesaria. De esta manera, solo podrá acordarse la medida: a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida.

[19] Este principio le exige al juez que valore si la prueba le va a ser útil para la investigación. Porque si la prueba resulta del todo prescindible no es idónea.

[20] Este principio le exige al juez estudiar en cada caso, sí la lesión a los derechos fundamentales que se ocasionaría con la medida de investigación a una persona es compensada con un mayor beneficio social producto de la autorización de la medida. Sí, del estudio resulta que el sacrificio del derecho fundamental frente al beneficio social es desproporcionado, el juez no podrá decretar la medida. De esta manera, las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes.

...*Ius puniendi* del Estado...

Desde una perspectiva de derecho comparado, vale la pena destacar que la dinámica de investigación de los países participantes coincide con el modelo de límites al ejercicio del *Ius puniendi* del Estado; esto es así en la medida que la incursión a la marcada tendencia de transición a sistemas de corte acusatorio en el contexto de sociedades democráticas donde la dignidad humana constituye un hito que configura la lógica funcional de sus instituciones, exige el respeto a los principios de reserva legal y reserva judicial.

Lo anterior quiere decir que la limitación intensa a derechos fundamentales siempre debe estar prevista de manera previa en la legislación positiva y debe provenir de un mandato judicial proferido por autoridad competente. En este entendido, en países como Colombia se sigue un modelo con un juez de control de garantías que sirve como escrutador de todo acto que afecte garantías fundamentales en el desarrollo de sus actos de investigación.

1.2.1.2- Técnica investigativa en materia de delincuencia cibernética

En el ámbito de las medidas investigativas que utilizan medios tecnológicos cobra mucha importancia la utilización de dispositivos (micrófonos, cámaras, etc.) para la captación y grabación de comunicaciones orales. Es importante señalar la relevancia de la sentencia del Tribunal Europeo de Derechos Humanos (TEDH) del 31 mayo del 2005, caso Vetter contra Francia. Con este fallo se establece la regla por vía jurisprudencial consistente en la imposibilidad de utilizar micrófonos para interceptar comunicaciones si no hay una norma legal que contemple la medida, pues se vulnera el artículo 8 (el Derecho a la privacidad) del Convenio Europeo de Derechos Humanos de 1950.

En virtud de lo anterior, en España se aprueba la Ley Orgánica 13/ 2015, del 5 de octubre, de modificación de la Ley Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Como consecuencia de esta reforma, el artículo 588 quater a y siguientes de la Ley de Enjuiciamiento Criminal, contemplan que podrá autorizarse la colocación y utilización de dispositivos electrónicos que permitan la captación y grabación de las comunicaciones orales directas que se mantengan por el investigado, en vía pública o en un espacio abierto, en su domicilio o en otros lugares cerrados.

Esta posibilidad queda circunscrita a uno o varios encuentros concretos del investigado con otras personas y sobre cuya previsibilidad haya indicios puestos de manifiesto por la investigación. Esta concreción puede venir determinada por factores locativos, temporales o de los sujetos intervinientes. Será necesario además que la investigación tenga por objeto uno de los siguientes delitos: delitos dolosos castigados con pena con un límite máximo de, al menos, 3 años de prisión; delitos cometidos en el seno de un grupo u organización criminal; y delitos de terrorismo. Asimismo, los arts. 588 quinquies b y c de la Ley de Enjuiciamiento Criminal, permiten la utilización de dispositivos de seguimiento y de geolocalización.

Aunado a lo anterior, dentro del repertorio de técnicas investigativas con fines judiciales en el contexto de la ciberdelincuencia se aprecian aquellos de origen telemático. De manera puntual, en materia de obtención de la prueba digital cobra especial importancia la interceptación de comunicaciones. Esta se entiende como la captación en tiempo real del contenido y/o datos asociados de una comunicación, tanto de telefonía (fija o móvil) como de cualquier tipo de red de datos, sin interrumpir el curso de esta para la obtención de datos útiles para la investigación y prueba del delito. Siempre que esta medida se utiliza se afecta el derecho fundamental al secreto de comunicaciones.

En el ordenamiento jurídico español la regulación específica de esta medida está, a partir del 2015, en los artículos 588 ter (a) y subsiguientes, LECRIM. En el ámbito subjetivo

de esta institución investigativa procesal, el sujeto activo por regla general es el juez. En ese sentido, existe un principio de reserva judicial. Excepcionalmente, se permite en algunos estados, a la autoridad perteneciente al Ejecutivo, recurrir a esta medida investigativa cuando se trata de delitos de terrorismo.

En relación con el sujeto pasivo se pueden interceptar las telecomunicaciones de aquellos medios utilizados de manera habitual u ocasionalmente por el investigado; también se pueden interceptar los medios utilizados por terceros siempre que concurran los siguientes supuestos: (i) Que existe constancia de que el sujeto investigado se sirve de aquella para trasmitir o recibir información, o (ii) el titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad. Se pueden interceptar las telecomunicaciones de la víctima, los terminales o medios de comunicación cuando sea previsible un grave riesgo para su vida o integridad. Por último, también se pueden interceptar las comunicaciones cuando existe la utilización maliciosa por terceros, *routers* y ordenadores *zombies* o *botnets* sin consentimiento del titular.

Desde el punto de vista del ámbito objetivo, ¿cuáles son los delitos que pueden ser investigados por medio de las interceptaciones de comunicaciones?: depende de cada ordenamiento jurídico en particular. Por lo general, se establecen criterios como un mínimo de gravedad en la pena, el tipo de delito y otras circunstancias, o que exista una organización criminal. Y pueden ser intervenidos los terminales y los sistemas de comunicación.

En cuanto al tipo de información a la cual puede accederse, por regla debe ser la señalada en la resolución judicial y esta puede recaer sobre el contenido de las comunicaciones en las que participe el sujeto investigado como emisor o receptor, los datos electrónicos de tráfico, que son todos los que se generan cuando se establece un proceso de comunicación por la red de comunicaciones electrónicas, y los datos que se produzcan con el establecimiento o no de una comunicación. Para el caso específico del ordenamiento jurídico español, el trámite de la interceptación, procesalmente hablando, tiene unas fases: (i) Solicitud de autorización judicial para intervención de comunicaciones; (ii) una vez autorizada la intervención, la operadora envía la información al servicio central (SITEL) donde se almacena; y se recoge archivo con firma electrónica; (iii) el personal de la unidad de investigación accede al servidor (utilizando código de identificación de usuario y clave personal): se vuelcan los datos en DVD -(única versión original)-, y elabora informe (forma tradicional) que se entrega al juez competente.

De igual forma, en países participantes como Colombia, este particular acto investigativo se encuentra regulado de manera amplia a nivel legal y jurisprudencial, requiriendo la preexistencia de orden judicial de un juez de control de garantías luego de la ponderación de los intereses investigativos frente a las posibles afectaciones que se puedan originar en su ejecución.

De igual forma, en el trascurso de este espacio académico también se estudió la institución de los registros como medio de investigación, los cuales pueden recaer: (i) sobre dispositivos electrónicos[20] ,(ii) datos en la nube y (iii) registros remotos. En cada una de estas modalidades,

[21] Los dispositivos electrónicos son aquellos que convierten el lenguaje binario (0 y 1) a lenguaje alfabético, imágenes, audios, videos, etc. Pueden ser de gran variedad, aparatos electrónicos como teléfonos móviles, smartphone, tabletas, ordenadores, GPS. También pueden ser medios de almacenamiento: dispositivos USB, ZIP, DVD.

las personas vierten una gran cantidad de información sobre su vida, ya sea sobre aspectos de la vida sexual, familiar o económica, que en una eventual intromisión producto de una investigación pueden afectarse derechos fundamentales como la intimidad personal, secreto de comunicaciones, derecho a la autodeterminación informativa en el ámbito de la protección de datos. Como todos estos derechos están entrelazados, se imbrican mutuamente.

El Tribunal Constitucional Alemán ha construido -al igual que la jurisprudencia española-, un derecho fundamental de nueva generación denominado el derecho fundamental a la protección eficaz del entorno virtual del afectado, entorno que se materializa en el conjunto de informaciones de diversa índole que son de la persona y se encuentra almacenada en los dispositivos. Desde una perspectiva procesal, el acceso lícito al dispositivo puede darse a través de autorización juridicial -previa solicitud-, mediante resolución judicial motivada satisfaciendo los principios de idoneidad, especialidad, excepcionalidad y necesidad.

En ese sentido, siempre que materialice el principio de proporcionalidad puede proceder el acto investigativo por cualquier tipo de delito; así mismo puede darse de manera excepcional sin autorización judicial, en situaciones de urgencia[22] y necesidad[23] , la autoridad policial judicial acceda al dispositivo siempre cumpliendo el principio de proporcionalidad[24] con control judicial posterior. Y, por último, el acceso a la información se da por consentimiento del afectado que puede legitimar la injerencia. El consentimiento puede ser expreso o tácito, pero sobre todo debe ser informado, lo que quiere decir que la autoridad investigativa judicial debe informarle al investigado las consecuencias negativas que se derivan de permitir que la autoridad acceda a los dispositivos donde se encuentra su información.

[22] El Tribunal Constitucional Español mediante sentencia STC 115/2013 manifiesta que la urgencia en el acceso a los datos por parte de la autoridad policial sin autorización previa se suscita cuando surge la necesidad de averiguar la identidad de los sujetos que han sido sorprendidos cometiendo la conducta punible y huyen del lugar de los hechos.

[23] El Tribunal Constitucional Español mediante sentencia STC 115/2013, define que la necesidad del acceso a los datos por parte de la policía sin autorización previa consiste que el registro no pueda lograrse por otro medio menos gravoso.

[24] El Tribunal Constitucional Español mediante sentencia STC 115/2013, plantea que la proporcionalidad en el acceso a los datos por parte de la autoridad judicial sin autorización judicial previa consiste en que el acceso de la autoridad judicial debe ser una medida equilibrada, ponderada por derivarse de ella más benéficos o ventajas para el interés general que prejuicios sobre otros bienes o valores.

[25] En España el 88% de las personas utiliza Whatsapp, el 87% Facebook, el 68% Youtube, el 54% Instagram, el 50% Twitter, LinkedIn el 25%, Pinterest el 20%, Telegram el 18% y el 7% de las personas utiliza Snatchap.

...en el ordenamiento jurídico español existe la figura del ciber patrullaje. El policía puede investigar apoyado en las redes sociales, crear un perfil falso y navegar y obtener información del investigado a distancia...

Por tanto, teniendo en cuenta los supuestos hasta hora vistos, si se da un registro ilícito, es decir, que no se encauza dentro de las circunstancias señaladas, es nulo de pleno derecho y no tienen ningún efecto en el proceso. En ese sentido, la sentencia no podrá fundamentarse en datos que podrían resultar del acceso ilícito a datos, ni en las percepciones de los sujetos que hubieran intervenido en la actuación de acceso ilícito, así como en los resultados que se deriven de esas pruebas de acceso ilícito. Como es una nulidad de pleno derecho, no puede ser subsanada y no ser incorporada al proceso.

Finalmente, en el ordenamiento jurídico español existe la figura del ciber patrullaje. El policía puede investigar apoyado en las redes sociales, crear un perfil falso y navegar y obtener información del investigado a distancia. Hasta ese momento todo es lícito y no se necesita autorización judicial. En el momento en que el investigado logra interacción y empieza a comunicarse con el investigado a través de su perfil, esas interlocuciones y comunicaciones deben ser autorizadas previamente. En el ordenamiento jurídico español se denomina agente encubierto virtual, que se utiliza fundamentalmente para investigar y desarticular redes de pederastia, terrorismo internacional, etc.

1.2.2
Manejo de la prueba digital en el contexto del cibercrimen

1.2.2.1- Fuentes probatorias en materia de cibercrimen

En materia probatoria se abordó el estudio de la prueba digital, la cual se definió como toda información producida, almacenada o transmitida por medios electrónicos con efectos para acreditar hechos en el proceso: informaciones contenidas en celulares, GPS (Sistema de Posicionamiento Global), smartphone, computadores, etc.

Esta prueba digital, tienen cuatro fuentes: (i) interceptación de comunicaciones (ii) registros de dispositivos (iii) fuentes abiertas y (iv) datos en proveedores de servicio. En este ámbito se hace necesario interrogarnos: ¿Dónde están los datos? Y estos se encuentran en los dispositivos electrónicos, que pueden ser utilizados por el autor del delito, el utilizado por la víctima o por terceros. También se encuentran en los proveedores de servicios y en la Web.
Cada fuente de la prueba digital u origen de la prueba digital tiene una institución procesal que nos permite acceder a los datos en la investigación y posteriormente utilizarlos como prueba en un proceso. En ese sentido, si materialmente la autoridad, de manera legítima, tiene en su poder un dispositivo electrónico, la institución procesal para acceder a ellos es el Registro de Dispositivos. En este punto es menester señalar que es posible que el dispositivo contenga múltiples aplicaciones que permitan conocer datos que se encuentra en la nube, por ejemplo: la aplicación del banco correspondiente, la aplicación de Amazon para compras; la institución procesal para acceder a esos datos es el Registro de Información Accesible. También es posible acceder al contenido del dispositivo a distancia, cuando no lo tenga en su poder la autoridad investigativa judicial, mediante un Registro Remoto.

Por otro lado, se puede acceder al contenido de los datos cuando se están trasmitiendo por las redes de comunicación. Cuando en tiempo real se está sucediendo una comunicación, este acceso se realiza mediante la interceptación de comunicaciones. Asimismo, los datos pueden estar en poder de los prestadores de servicio: Movistar, Claro, etc.

En algunas situaciones, dependiendo de la legislación positiva de cada país, las empresas están obligadas a conservar determinados datos a disposición de la autoridad judicial, exigencia que se denomina: Obligación de Conservación. Ahora bien, como esos datos están en poder de los prestadores de servicio y, por lo general, se destruyen cada cierto tiempo, la autoridad puede necesitarlo para bienes forenses, lo cual hace necesario la existencia de la institución judicial de orden de congelación. Finalmente, los datos se encuentran en la Web, en la cual encontramos fuentes abiertas, aunque también puede haber fuentes cerradas cuando nos encontramos con procesos de comunicación.

En material procesal, se puede acceder a todos los datos digitales, pero se hace necesario cumplir con determinados principios:

Principio de especialidad:

La medida a solicitar debe ser para investigar un delito concreto o varios delitos concretos. No se podrán autorizar medidas de investigación tecnológica que tenga por objeto prevenir o descubrir delitos o despejar duda sin base objetiva.

Principio de idoneidad:

La medida tiene que servir para aportar datos útiles a la investigación y prueba.

Principio de excepcionalidad y necesidad:

De conformidad con el artículo 588 bis (a) LECRIM: "solo podrá acordarse la medida: a) cuando no estén a disposición de la investigación, en atención a las características, otras medidas menos gravosas para los derechos fundamentales del investigado y encausado e igualmente útiles para el esclarecimiento del hecho o (b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a estas medidas.

Principio de proporcionalidad:

Las medidas de investigación reguladas se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e interés afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación del interés en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social, o el ámbito tecnológico de la producción y la intensidad de los indicios.

En materia de registro de datos se abordó la temática del acceso de datos en la nube, que se realiza mediante un registro ampliado. ¿Cuándo ocurre esto? Cuando la policía, la fiscalía o el Juez de Intrusión tiene materialmente un ordenador, un celular o un smartphone, y en estos existen aplicaciones que permiten a la persona (el tenedor o dueño) ingresar a aplicaciones de acceso a datos almacenados o existentes en la nube (por ejemplo, Amazon, la entidad financiera o a sus redes sociales. La fiscalía, la policía o el juez pueden acceder a estos datos, que están en esas aplicaciones o en la nube, en los siguientes supuestos:

- Si el dispositivo está abierto y el acceso a su contenido es posible sin uso de claves y contraseña mediante el Registro de Información Accesible.

- Si la autoridad pública conoce las claves de manera legítima, ya sea porque fueron suministradas por su titular o por análisis forense se pueden acceder a los datos de la nube mediante Registro Accesible de Datos.

- Si el dispositivo está cerrado y no se conocen las claves para acceder a los datos de la nube se realiza un Registro Remoto.

Pero esta operación se complica cuando los datos no se encuentran en el territorio, toda vez que ellos reposan en servidores que generalmente están ubicados en otros países: Estados Unidos, Canadá, Irlanda etc. En el ordenamiento jurídico español se permite el acceso a los datos que están en la nube siempre y cuando el dispositivo se encuentre en territorio español. El régimen jurídico del Registro Accesible señala que debe haber una autorización judicial inicial al dispositivo. Ahora bien, si se encuentra que en el dispositivo hay una aplicación que permite acceder a datos en la nube, debe haber una autorización judicial sobrevenida que expresamente diga que se pude acceder a esos datos que reposan en la nube.

El Registro Remoto consiste en la utilización de datos de identificación y códigos que, mediante la instalación de un software, permita de forma remota y telemática el examen a distancia -sin consentimiento de su titular o usuario- del contenido del ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos. El régimen jurídico de esta institución investigativa es mucho más estricto, pues su utilización implica una intromisión grave a los derechos fundamentales. En el ordenamiento jurídico español solo es posible recurrir al Registro Remoto en algunos de los siguientes delitos, previa autorización judicial (Reserva Judicial):

- Delitos cometidos en el seno de organizaciones criminales.

- Delitos de terrorismo.

- Delitos cometidos contra menores o con capacidad modificada judicialmente.

- Delitos contra la constitución, de traición y relativos a la defensa nacional.

- Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

En lo concerniente a los proveedores de servicios, teniendo en cuenta el Convenio de Budapest, se maneja un concepto amplio que abarca: (i) servicios de acceso a internet; (ii) servicios de comunicaciones electrónicas interpersonales; (iii) servicios de la sociedad de la información; (iv) servicios de infraestructura de internet. Los datos que reposan en los proveedores de servicios pueden clasificarse de manera tradicional en: datos de suscripción, datos de tráfico, datos de contenido. La clasificación es importante porque debe tenerse en cuenta al realizar el juicio de proporcionalidad cuando el juez autorice el acceso a los datos que están en poder de los proveedores de servicio.

Ahora bien, ¿Cuáles son esos datos?: datos de abonado (identidad del abonado o cliente, el tipo de servicio y su duración), datos relativos al acceso (datos relativos al inicio y final de una sesión de acceso al usuario a un servicio, la dirección IP asignada al usuario por el proveedor de servicios); datos de transacciones (datos de transacciones relacionadas con la prestación de un servicio ofrecido por un proveedor de servicios que sirvan para facilitar información contextual o adicional sobre dicho servicio y sean generados o tratados por un sistema de información del proveedor del servicio, tales como origen o destino del mensaje, la ubicación del dispositivo, la fecha la hora, la duración, el tamaño, la ruta el formato, etc); y datos de contenido (todo dato almacenado en formato digital como textos, voz, sonidos, vídeos, imágenes y sonidos, distinto de los datos de los abonados, los datos relativos al acceso o los datos de transacciones).

Como se dijo anteriormente otra fuente de datos y, por consiguiente, fuente de prueba digital, son las llamadas Fuentes Abiertas: motores de búsqueda, páginas y sitios web[26] y redes sociales. Con relación a los motores de búsqueda y sitios web no necesitan autorización judicial para acceder a esos datos ya que se encuentran libremente en la red. Por regla general, acceder a los datos que circulan libremente en las redes sociales de una persona no amerita autorización judicial para acceder a ellos. No obstante, hay que precisar particulares situaciones en la cuales, en el marco de las redes sociales, sí se necesitaría autorización judicial.

[26] La web puede ser clasificada en: Surface web, Deep Web y Dark web. La Surface web es la parte de internet con la que cotidianamente trabajamos y navegamos con motores de búsqueda como Bing, Google, etc. La Deep Web es el contenido de internet que no es especializado y a la cual solo se puede acceder con un software especializado, mientras que la Dark Web, es la parte de internet donde todo es anónimo y está cifrado siempre y solo se puede acceder a través de un router o protocolo especifico.

fuente de datos abiertas|

Como se dijo anteriormente otra fuente de datos y, por consiguiente, fuente de prueba digital, son las llamadas Fuentes Abiertas: motores de búsqueda, páginas y sitios web y redes sociales.

1.2.2.2- Cadena de custodia en materia de cibercrimen

Una vez estudiados y detallados los medios de investigación en materia de ciberdelincuencia, desde el punto de vista procesal, y una vez obtenidos los datos y las informaciones que van a ser prueba en el proceso se hizo imprescindible estudiar la Cadena de Custodia en Registro de Dispositivos. La cadena de custodia, como institución procesal, consiste en el procedimiento, oportunamente documentado, que permite constatar la identidad, integridad y autenticidad de los vestigios o indicios de un hecho relevante para el asunto (proceso), desde que son encontrados hasta que se aportan al proceso como pruebas.

Este concepto de cadena de custodia es aplicable a los datos que se obtienen de los dispositivos siempre y cuando se cumpla dos requisitos: la autenticidad y la integridad. La autenticidad en materia de cadena de custodia de prueba electrónica o digital consiste en que se garantiza la calidad del origen de los datos, es decir, se garantiza la fuente de la que proceden los datos. Mientras que la integridad es la propiedad consistente en que los datos no han sido alterados de manera no autorizada.

En este punto, lo importante en el Registro de Dispositivos es el volcado o clonado en el cual se realiza una copia espejo bit a bit de la información original que se toma mediante una herramienta *hardware* de tal manera que se realiza una copia física del contenido. Esta copia tiene un código un código hash que se calcula a partir de un algoritmo que permite acreditar que los datos hallados en los dispositivos no han sido alterados. Este volcado o clonado de datos puede realizarse cuando se aprehende el soporte o después durante el registro o posteriormente. Por otra parte, este volcado o clonado debe garantizarse técnica y jurídicamente: la primera consiste en que se deben utilizar instrumentos tecnológicos y procedimientos estándares/ homologación en el clonado de datos y la segunda, hace referencia a que este volcado de datos deber hacerse en presencia de testigos o federatio público.

1.2.3 Mecanismos de cooperación internacional y dimensión trasnacional de la prueba digital

De mucha importancia en el curso sobre ciberdelincuencia fue la reflexión en torno a la prueba digital internacional, que tuvo como origen del estudio, en materia de prueba digital, la siguiente pregunta: ¿Qué puede solicitarse a las autoridades extrajeras? La respuesta a este cuestionamiento consistió en que se pueden pedir dos cosas: (i) obtención de datos en tiempo real de una comunicación (interceptación de comunicaciones) y (ii) remisión de datos almacenados (datos que están en poder de los proveedores de servicios de comunicación que están en otro país). Lo anterior se logra a través de los canales o vías de la Cooperación Penal Internacional, la cual tiene el siguiente esquema:

1. Existe un proceso penal en el país requirente, en el cual se requiere la información. Necesidad de Resolución Judicial admitiendo la prueba digital con base a las normas nacionales del país.

2. Solicitud a la autoridad judicial extrajera, en los términos que está establecido en el particular Convenio de Cooperación Internacional.

3. Actuación de la autoridad extranjera requerida. Esta se realiza con base en el ordenamiento - (Lex Loci)-, jurídico de la autoridad extrajera requerida,

4. Validez en el país requirente de lo actuado.

Centrándonos en el numeral (4), al preguntarnos cuál es la validez de la prueba digital que proviene del extranjero, en el curso sobre ciberdelincuencia se señaló que dependerá de las normas del derecho positivo de cada país. En España en particular, la prueba -obtenida en el extranjero de conformidad a las normas del país de la cual proviene-, es válida en el país ibérico. También se puede valorar si la prueba se practicó conforme a las normas del país de donde proviene: la inobservancia ha de ser probada por quien la alega. Así mismo, se puede valorar si en el país de ejecución se han mantenido unas garantías sustancialmente similares a las exigidas en España para la restricción de los derechos de los ciudadanos en virtud de la jurisprudencia STS 1099/2015.

Para lo anterior, solo se debe aportar un dato objetivo sugestivo de una posible infracción de derechos fundamentales y debe ser alegado por quien lo desee hacer valer.

En lo relacionado con mecanismo de Cooperación Internacional concretos, podemos señalar la Cooperación Judicial Civil (convenios bilaterales y multilaterales): Convenio de La Haya del 18 de marzo de 1970, relativo a la obtención de pruebas en material civil y mercantil en el extranjero; Convención Interamericana sobre exhortos o cartas rogatorias, suscrito en Panamá el 30 de enero de 1975; en la Unión Europea existe el Reglamento (CE) 1206/2001 del 28 de Marzo del 2001, relativo a la Cooperación de los órganos jurisdiccionales de los Estados miembros en el ámbito de la obtención de pruebas en materia civil y mercantil.

En materia de Cooperación Penal Internacional los convenios bilaterales por lo general no consagran normas específicas sobre prueba digital, aunque es posible destacar varios convenios multilaterales en materia penal. El artículo 18 de la Convención de Palermo: Convención de las Naciones Unidas contra la delincuencia Organizada Transnacional; Convenio de Budapest: Convenio Europeo Sobre la Ciberdelincuencia del año 2001; el Tratado de Madrid en Iberoamérica de 2014 y, finalmente, en la Unión Europea existe la Orden Europea de Investigación.

El Sistema del Convenio de Budapest del año 2001, que nace en el seno del Consejo de Europa, ha trascendido los límites regionales europeos y ha sido ratificado por países que no forman parte del Consejo de Europa: Argentina, Japón, Republica Dominicana, Chile, Panamá, Colombia, Perú, Paraguay, Estados Unidos, Canadá, entre otros. Este convenio puede ser utilizado para la aplicación de asistencia mutua en: (i) delitos Informáticos, y (ii) la obtención de pruebas electrónicas de un delito. El sistema del Convenio de Budapest contempla la obtención en tiempo real de datos -asociados o contenidos- que estén en el Estado requerido, así como la remisión de datos almacenados en poder de un proveedor de servicios que está en el Estado requerido: conservación[27], remisión[28], acceso transfronterizo de datos[29].

[27] En virtud del convenio, por ejemplo, Perú puede solicitarle a Panamá que le ordene a un proveedor de servicios informativos y de telecomunicaciones que conserve los datos que Perú va necesitar. Esto se denomina la Conservación rápida de datos almacenados. Esta, es previa a la solicitud de Registro o Acceso, confiscación o revelación de datos. También contempla el Convenio de Budapest, la revelación rápida de datos conservados, consistente en que, si un país solicita a otro la conservación de unos datos que están en poder de un proveedor de servicios que está en su territorio, pero el país requerido llega al conocimiento que los datos se encuentran en un proveedor de servicios que se encuentra en otro país, el país requerido debe informarlo al país requirente.

[28] Consiste en que una vez conservados los datos por el país requerido donde se encuentra el proveedor de servicios, la parte requirente puede solicitar a la parte requerida que acceda, registe, confisque u obtenga de forma similar, datos informáticos por medio de un sistema informático situado en el territorio de la parte requerida.

[29] En esta institución, la autoridad de un país puede acceder a datos que están en poder de los proveedores de servicios que están en otro país, sin la autorización de este último en dos situaciones: tener acceso a datos informáticos almacenados que se encuentren a disposición del público (Fuente Abierta); tener acceso o recibir, a través de un sistema informático situado en su territorio, datos infor-

En el contexto Iberoamericano en materia de cooperación penal internacional, es importante el Tratado de Madrid: Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de la Prueba en materia de Ciberdelincuencia, del 28 de mayo del 2014. Este ha sido firmado por Guatemala, Nicaragua, Portugal, Perú y Uruguay (aunque todavía no ha entrada en vigor dado que todavía no cuenta con la ratificación de tres Estados que es necesaria para dicha vigencia). Tiene como objeto reforzar la cooperación mutua de las partes para la adopción de medidas de aseguramiento y obtención de pruebas para la lucha contra la ciberdelincuencia.

En el ámbito de medidas de aseguramiento el presente tratado regula lo siguiente:

1. La incautación y depósito de sistemas informáticos o soportes de almacenamiento de datos.

2. El sellado, el precinto y prohibición del uso de sistemas informáticos o soportes de almacenamiento de datos.

3. El requerimiento de preservación inmediata de datos que se hallan en poder de terceros.

4. La copia de datos.

En materia de diligencias de investigación, el Tratado de Madrid regula lo siguiente:

1. La intervención de comunicaciones a través de las tecnologías de la información y comunicación.

2. La obtención de datos de tráfico.

3. El acceso a sistemas de información.

4. Acceso a la información contenida en un dispositivo que permita el almacenamiento de datos.

5. La entrega de datos y archivos informáticos.

En el contexto de la Unión Europea, la Prueba Digital Internacional tiene que tramitarse a través de la Orden Europea de Investigación (OEI), la cual está regulada en la Directiva 2014/41/CE, transpuesta en el ordenamiento español mediante en la Ley 23/2014, reformada por la Ley 3/2018. Este sistema se basa en la idea de reconocimiento mutuo de resoluciones judiciales, y consagra una serie de posibilidades en materia de investigación de ciberdelitos: interceptación de comunicaciones, preservación de datos y remisión de datos.

En la actualidad hay una propuesta de reglamento sobre ordenes europeas de producción y preservación de evidencias electrónicas en materia criminal. En el curso sobre ciberdelincuencia se hizo énfasis en la importancia que está asumiendo la evidencia electrónica en los procesos penales, ya que está presente en numerosos supuestos. Panorama que cobra complejidad, puesto que muchos proveedores de servicios que se encuentran fuera del territorio nacional (particularmente en Estados Unidos), donde la mayoría de las empresas como Facebook y Twitter manejan sus propios protocolos de privacidad.

Como estrategia para conjurar esta situación, desde el curso se formularon las siguientes recomendaciones:

(i) agotar fuentes abiertas y recursos internos

(ii) solicitud Internacional alternativa a la comisión rogatoria: solicitud directa al proveedor de servicios que se encuentra en otro país, mecanismos de cooperación policial, etc;

(iii) y, por último, el uso de asistencia judicial internacional.

la evidencia electrónica|

En la actualidad hay una propuesta de reglamento sobre ordenes europeas de producción y preservación de evidencias electrónicas en materia criminal. En el curso sobre ciberdelincuencia se hizo énfasis en la importancia que está asumiendo la evidencia electrónica en los procesos penales, ya que está presente en numerosos supuestos.

2

CONCLUSIONES Y RECOMENDACIONES

Una vez transitada nuestra atención por los diferentes acápites de este esfuerzo mancomunado entre los países participantes debemos llamar la atención del lector en los siguientes puntos de reflexión:

En primer lugar, resulta evidente la necesidad de llamar la atención de los responsables de perfilar la política criminal en cada país sobre la incidencia y potencial dañino de aquellos fenómenos asociados con la cibercriminalidad. Esto por cuanto en la mayoría de los ordenamientos jurídicos penales no existe un título destinado al abordaje especializado de los principales ciberdelitos.

En compensación de lo anterior existen tipificaciones de conductas que se pueden catalogar como modalidades de ciberdelincuencia económica o intrusiva, pero en títulos donde se tipifican delitos contra el patrimonio económico, la integridad o formación sexual, etc.

En ese orden de ideas resulta una prioridad armonizar la normatividad interna de cada país con los avances registrados desde la óptica del derecho comparado, partiendo de la especial referencia del Convenio de Budapest del 23 de noviembre de 2001.

En segundo lugar, dado al amplio desarrollo del crimen organizado en materia de delincuencia cibernética económica e intrusiva se debe establecer como meta la adecuación de las legislaciones procesales para la adopción de la figura del agente encubierto virtual, en los correspondientes acápites sobre investigación criminal, pues esta es la única manera de ofrecer una respuesta adecuada a este tipo de fenómenos.

En tercer lugar, es necesario fortalecer los mecanismos de cooperación penal internacional en atención como medida pertinente e idónea para hacer frente a la naturaleza transnacional de este tipo de delincuencia de incidencia global.

En cuarto lugar, se requiere el fomento y fortalecimiento de los espacios de capacitación, tanto de los equipos de policía judicial como de los funcionarios o agentes encargados de la persecución penal y la administración de justicia en materias poco desarrolladas a nivel legislativo como lo es el manejo de la cadena de custodia y la prueba digital.

Lo anterior además, como una forma de garantizar en la mejor medida posible las garantías fundamentales de todos aquellos sujetos que puedan ser objeto de pesquisas investigativas por parte del Estado.

En quinto lugar, en la mayoría de los países participantes existen medidas de investigación tecnológicas que tienen que ser solicitadas por la fiscalía o el ministerio fiscal al Juez de Control de Garantías, las cuales una vez decretadas tienen control posterior por este último. Sin embargo, existen otros países participantes en los que estas medidas de investigación con medios tecnológicos no existen en sus legislaciones procesales penales. Las recomendaciones en este ámbito van encaminadas a consagrar estas medidas para poder preservar el Estado de Derecho y los derechos fundamentales de las personas.

En sexto lugar, consecuentemente con la ausencia de legislación penal especializada en materia de ciberdelincuencia en la mayoría de países participantes, se destaca el hecho de la poca o ausente reglamentación y desarrollo en materia de policía judicial especializada para estos temas de complejo abordaje. Se recomienda un fortalecimiento en la aprehensión de estas técnicas investigativas y la inversión en los equipos necesarios para su correcta función.

3
FICHAS POR PAÍSES

¿Tipifica su país bajo un título, capítulo, los ciberdelitos?

La República Argentina no tipifica de manera sistemática bajo un mismo título los delitos informáticos o ciberdelitos. A partir del año 2008 se sanciona la Ley 26.388 de delitos informáticos y Argentina adaptó su legislación al "Convenio sobre Cibercriminalidad" -Budapest en el año 2001- , que importó una modificación al Código Penal, incluyendo los delitos informáticos y sus penas de manera dispersa en los diferentes títulos que lo integran, de conformidad con los bienes jurídicos principalmente afectados.

Así mismo, con la Ley 26.904 incorporó la figura penal del grooming. De igual forma con la sanción de la Ley 27.411 a fines de 2017, Argentina aprueba parte de la Convención de Budapest y con ello asume el compromiso internacional de adecuar su normativa interna a fin de facilitar la investigación de los denominados delitos. Sin embargo, con esta adhesión a la Convención se efectuaron diversas reservas en varios tópicos dentro de las cuales se destaca:

1- Reserva en canto a la tipificación de actos preparatorios (art. 6.1.b del Convenio de Budapest). Debe recordarse que este precepto castiga la posesión de dispositivos o software para permitir la comisión de otros delitos; o la tenencia de códigos de acceso que permitan acceder a un sistema informático, en ambos casos con la intención de utilizarlos para cometer un delito. Nuestro sistema penal enmarca esta clase de actos en el plano de la tentativa criminal.

2- Reservas por tratarse de figuras incompatibles con el Código Penal. Por ejemplo, en el art. 9.1 "d" del Convenio en cuanto castiga "el hecho de procurarse pornografía infantil a través de un sistema informático" incrimina al visualizador o adquirente, y esta acción per se no está prevista en la legislación argentina como acción punible. Luego en relación al art. 9.2 de la Convención, al definir que debe entenderse por pornografía infantil: en Argentina solo se considerará pornografía infantil la que involucra a un menor adoptando un comportamiento sexualmente explícito, no así los otros supuestos que prevé ese artículo.

3- Reserva parcial en relación al concepto de tenencia de pornografía infantil. En Argentina, esta tenencia será punible cuando se demuestre que se almacena con fines inequívocos de distribución o comercialización.

4- Reserva respecto a las reglas de competencia penal, ya que nuestro país no acepta por principio ni la aplicación extraterritorial de la ley penal, ni la jurisdicción personal.

5-Finalmente, reserva en cuanto a los compromisos de cooperación internacional. Se requiere para colaborar en la conservación o resguardo de los datos, que el delito en cuyo marco se piden estas medidas, sea delito tanto en el Estado que solicita la colaboración como en el que cuya colaboración se requiere.

Como consecuencia del ingreso a la Convención, Argentina creó la "Unidad 24/7 de Delitos Informáticos y Evidencia Digital que asumirá las funciones como punto de contacto de la Red 24/7.

Argentina

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

Se contempla la estafa informática mediante el artículo 173 inciso 16. También se contemplan los delitos de robo, hurto y daños a objetos informáticos.

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

Argentina incorpora a través de las leyes 26.388 (Ley de Delitos Informáticos); 26.904 (grooming) y 27.436 (penaliza la tenencia de pornografía infantil)

¿Tiene su legislación procesal penal medidas restrictivas de internet (bloqueo, retiro de páginas web, etc.) en materia de ciberdelincuencia económica e intrusiva?

No lo contempla. Se puede lograr bloqueo o retiro de publicaciones por medio de una medida cautelar, pero a instancia de un interesado que acredite interés legítimo.

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización judicial? ¿Cuál? y ¿Por qué no la exige?

No informa

¿Cuáles son las medidas concretas de investigación con medios tecnológicos que contempla la legislación penal de su país?

En el CPP CABA se encuentra previsto el uso de medios tecnológicos para controlar y garantizar la efectividad de las medidas de protección dispuestas respecto de las víctimas (botones antipánico con gps), para el control de las medidas restrictivas impuestas al imputado, de las reglas de conducta establecidas respecto de un probado o condenado en suspenso, o para contralor de la detención domiciliaria o de la efectivización de una medida de seguridad. Por otra parte, no hay impedimento legal para la utilización de micrófonos como medida de investigación o de herramientas de geolocalización, dependiendo que exista autorización judicial, y que su aplicación se adecue a los principios de necesidad, razonabilidad, subsidiariedad y proporcionalidad.

En la Ciudad de Buenos Aires, el CPP (Ley 2303), autoriza a la requisa y secuestro, entre otras cuestiones de equipos de computación u otro soporte informático, por orden del fiscal o del juez, en este último caso si se trata de los elementos mencionados en el artículo 13.8 de la Constitución local ("el allanamiento de domicilio, las escuchas telefónicas, el secuestro de papeles y correspondencia o información personal almacenada").

En casos urgentes, la medida puede ser delegada en la autoridad policial. La interceptación de correspondencia tiene que ser pedida por el fiscal al Juez de Garantías.

También prevé medidas especiales de investigación, pero no específicamente de carácter tecnológico. Contempla el agente encubierto, por ejemplo, pero no alude específicamente al agente encubierto informático, aunque se puede interpretar que se encuentre comprendido en la figura. En definitiva, en todos los casos, toda medida intrusiva debe ser con orden judicial.

¿Pueden los particulares y detectives o investigadores privados utilizar medidas tecnológicas de investigación sin autorización judicial y en qué supuestos?

No informa

¿Existe en su país una normativa que regula específicamente las medidas de investigación tecnológica restrictivas de derechos fundamentales y cómo la valora?

Art. 151, Ley 27.063, art. 152, Ley 27.063

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

No informa

¿Quiénes pueden solicitar y decretar estas medidas?

Las solicita el Fiscal y las decreta el Juez. Pero solo la interceptación telefónica, las demás están sujetos al principio de libertad probatoria.

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

No informa

¿Es necesario autorización judicial para colocar una baliza en su país? ¿Hay regulada la posibilidad de utilizar judicialmente otras herramientas de geolocalización? En caso afirmativo, explique brevemente los requisitos exigibles.

No informa

¿Cómo valora la normativa interna de su país relativa a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos (celulares, tablets, computadoras...)?

No informa

¿Qué valor se otorga en su país a la prueba digital (e-evidence) obtenida por Comisión Rogatoria Internacional?

No informa

En su país, ¿es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional?

No informa

¿Considera adecuada la legislación de su país sobre obligación de conservación de datos por las operadoras de comunicación para la investigación y prueba de los delitos?

Es insuficiente

¿Tipifica su país bajo un título, capítulo, los ciberdelitos?

La normatividad boliviana a través de la Ley No. 1768 modificó su Código Penal introduciendo el capítulo XI sobre delitos informáticos las siguientes figuras típicas:

Artículo 363 bis. - (Manipulación informática). - El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal, cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

Artículo 363 ter. - (Alteración, acceso y uso indebido de datos informáticos). - El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

No contempla la legislación boliviana ciberdelito económico. Existe un tipo penal abierto sobre manipulación informática utilizado para cubrir algunos vacíos frente a conductas o infracciones que afectan varios intereses objeto de tutela por medio del uso de herramientas digitales.

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

La legislación boliviana contempla el delito descrito en el artículo 363 ter como Alteración, Acceso y Uso Indebido de Datos Informáticos, cuya alcance y presupuestos objetivos se compagina con la naturaleza de ciberdelitos intrusivos.

¿Tiene su legislación procesal penal medidas restrictivas de internet (bloqueo, retiro de páginas web, etc.) en materia de ciberdelincuencia económica e intrusiva?

No existe regulación legal al respecto de esta materia en el Código Procesal Penal, ni en el Código Penal para el caso de ciberdelincuencia económica.

En el caso de ciberdelincuencia intrusiva, la Ley Nº 348 del 2013 contempla medidas de protección frente a la violencia mediática en el contexto de la violencia de género, definiendo la violencia mediática como: "Es aquella producida por los medios masivos de comunicación a través de publicaciones, difusión de mensajes e imágenes estereotipadas que promueven la sumisión y/o explotación de mujeres, que la injurian, difaman, discriminan, deshonran, humillan o que atenían contra su dignidad, su nombre y su imagen.

¿Cuáles son las medidas concretas de investigación con medios tecnológicos que contempla la legislación penal de su país?

No existe regulación legal al respecto de esta materia en el Código Procesal Penal, ni en el Código Penal.

¿Quiénes pueden solicitar y decretar estas medidas?

De conformidad con el artículo 191 del CPP, es el juez quien se encuentra facultado para adelantar cualquier acto de investigación de esta naturaleza invasiva de otros derechos. Partiendo de la premisa de que toda información a recolectar pueda ser considerado como documento se tiene que la norma señala:

"Artículo 191º.- (Apertura y examen). Recibida la correspondencia, documentos o papeles, el juez o tribunal en presencia del fiscal procederá a su apertura y examen debiendo constar en acta. Si guardan relación con el proceso, ordenará el secuestro; caso contrario, mantendrá en reserva su contenido y dispondrá su entrega al destinatario o remitente o a su propietario."

¿Pueden los particulares y detectives o investigadores privados utilizar medidas tecnológicas de investigación sin autorización judicial y en qué supuestos?

No puede, se genera prueba ilícita, no existe ningún supuesto al respecto.

¿Existe en su país una normativa que regula específicamente las medidas de investigación tecnológica restrictivas de derechos fundamentales y cómo la valora?

No existe.

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

No informa.

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización judicial? ¿Cuál? y ¿Por qué no la exige?

No existe.

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

No, está por prohibido por la Constitución Política del Estado en su artículo 25.

¿Es necesario autorización judicial para colocar una baliza en su país? ¿Hay regulada la posibilidad de utilizar judicialmente otras herramientas de geolocalización? En caso afirmativo,

No está contemplado en la legislación.

¿Cómo valora la normativa interna de su país relativa a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos (celulares, tablets, computadoras...)?

No está contemplado en la legislación.

¿Qué obstáculos se encuentran cuando la autoridad judicial de su país ha de acceder a los datos de un proveedor de servicios que está situado en otro Estado?

Es muy complejo por factores de toda índole tales como deficiencias en el servicio de traductores; además, difícilmente llegan las respuestas a lo solicitado.

¿Qué valor se otorga en su país a la prueba digital (e-evidence) obtenida por Comisión Rogatoria Internacional?

Tiene el mismo valor que un documento de sujeta a reglas de valoración de conformidad con el artículo 173 CPP. Que señala:

"El juez o tribunal asignará el valor correspondiente a cada uno de los elementos de prueba, con aplicación de las reglas de la sana crítica, justificando y fundamentando adecuadamente las razones por las cuales les otorga determinado valor, en base a la apreciación conjunta y armónica de toda la prueba esencial producida."

En su país, ¿es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional?

No. Todo es por cancillería.

¿Considera adecuada la legislación de su país sobre obligación de conservación de datos por las operadoras de comunicación para la investigación y prueba de los delitos?

No informa.

¿Tipifica su país bajo un título, capítulo, los ciberdelitos?

No lo contempla de manera expresa.

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

De manera expresa la legislación brasilera no contempla figuras típicas encaminadas a describir conductas que congloben la ciberdelincuencia como un fenómeno delictivo autónomo; sin embargo, para cubrir esas falencias en la práctica se dispone de los delitos tradicionales cuyas descripciones contemplan presupuestos abiertos o circunstancias especiales compatibles con la naturaleza de estos comportamientos, tales como el hurto electrónico descrito en el artículo 155, §§ 4º-B e 4º-C, del Código Penal y el fraude electrónico en el artículo 171, §§ 2º-A e 2º-B, del Código Penal. Incluso, en materia de derecho de propiedad intelectual e industrial, las normas del Código Penal permiten adecuar dentro de sus presupuestos aquellos atentados que se realice sobre medios electrónicos.

¿Tiene su legislación procesal penal medidas restrictivas de internet (bloqueo, retiro de páginas web, etc.) en materia de ciberdelincuencia económica e intrusiva?

En Brasil, el bloqueo, inacceso o retirada de contenidos está gobernado por una ley específica como lo es el Marco Civil de Internet. Esa ley puede ser aplicada por el juez penal si lo pide el fiscal o la víctima, permitiendo ordenar la retirada de contenido al proveedor de servicios en internet.

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

La legislación brasilera regula de manera expresa en su Código Penal el delito de invasión de dispositivo informático en el artículo 154-A, contemplando incluso la figura del espionaje informático de secretos empresariales en el Art. 154-A, § 3º; en el artículo 266 el delito de interrupción o perturbación del servicio telegráfico, radiotelegráfico o telefónico.

Además de lo anterior, también se contempla los delitos de pornografía infantil, abuso sexual, y otras figuras como el child grooming y el acoso –stalking como componentes de delitos relacionados con limitaciones a la libertad personal en el Código Penal o estatutos especiales destinados a la tutela de derechos de adolescentes.

¿Cuáles son las medidas concretas de investigación con medios tecnológicos que contempla la legislación penal de su país?

En la legislación brasilera se contempla de manera puntual el uso de micrófonos; la infiltración de agentes de policía en internet para delitos de pornografía infantil así como delitos sobre bandas criminales; registro de datos de geolocalización; así mismo registro de datos, de conexión o acceso a aplicaciones de internet, además de datos personales y comunicaciones privadas almacenadas.

¿Quiénes pueden solicitar y decretar estas medidas?

Son autorizadas por el poder judicial, excepcionalmente la policía puede realizarlas directamente.

¿Pueden los particulares y detectives o investigadores privados utilizar medidas tecnológicas de investigación sin autorización judicial y en qué supuestos?

Las personas y los detectives o investigadores privados no pueden, por regla general, utilizar medidas de investigación tecnológica sin autorización judicial.

¿Existe en su país una normativa que regula específicamente las medidas de investigación tecnológica restrictivas de derechos fundamentales y cómo la valora?

Ley 9.296 / 96, Ley No. 13.964, 2019, Ley N ° 13.344 de 2016

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

Se aplica los criterios del juicio de proporcionalidad.

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización judicial? ¿Cuál? y ¿Por qué no la exige?

Existen medidas tecnológicas de investigación que pueden ser utilizadas y tienen validez probatoria sin depender de autorización judicial.

Sobre el particular, expresa el Art. 13-B., de ser necesario para la prevención y represión de delitos relacionados con la trata de personas, el miembro del Ministerio Público o el delegado policial podrá solicitar, mediante autorización judicial, a las empresas proveedoras de servicios de telecomunicaciones y / o telemática que proporcionen de manera inmediata los medios técnicos apropiados. - como letreros, información y otros - que permitan la ubicación de la víctima o sospechosos del delito en curso. (Incluido por Ley N ° 13.344 de 2016)

§ 1 A los efectos de este artículo, señal significa el posicionamiento de la estación de cobertura, sectorización e intensidad de radiofrecuencia. (Incluido por Ley N ° 13.344 de 2016)

Párrafo 2. En el evento a que se refiere la caput, el signo: (Incluido por Ley N ° 13.344, 2016)
I - no permitiré el acceso al contenido de la comunicación de cualquier naturaleza, que dependerá de la autorización judicial, según lo disponga la ley; (Incluido por Ley N ° 13.344 de 2016)

II - debe ser provisto por el proveedor de telefonía celular por un período no mayor de 30 (treinta) días, renovable una vez, por el mismo período; (Incluido por Ley N ° 13.344 de 2016)

III - para períodos superiores a los referidos en el punto II, será necesario presentar una orden judicial. (Incluido por Ley N ° 13.344 de 2016)

§ 3 En el caso previsto en este artículo, la investigación policial deberá iniciarse en el plazo máximo de 72 (setenta y dos) horas, contadas desde el registro del suceso policial respectivo. (Incluido por Ley N ° 13.344 de 2016)

Párrafo 4. De no existir manifestación judicial dentro de las 12 (doce) horas, la autoridad competente solicitará a las empresas proveedoras de servicios de telecomunicaciones y / o telemática que proporcionen de manera inmediata los medios técnicos apropiados - tales como señales, información y otros - que permitan la ubicación del víctima o sospechosos del delito en curso, con notificación inmediata al juez. (Incluido por Ley N ° 13.344 de 2016)

¿Cómo valora la normativa interna de su país relativa a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos (celulares, tablets, computadoras...)?

Se requiere orden judicial para todas las medidas de investigación tecnológica restrictivas de derechos fundamentales.

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

En Brasil, existe respaldo legal para el uso del micrófono como medida de investigación, como se transcribe a continuación de un extracto de la Ley 9.296 / 96:
Art. 8-A. Para investigación o instrucción criminal, la captura ambiental de señales electromagnéticas, ópticas o acústicas podrá ser autorizada por el juez, a solicitud de la policía o del Ministerio Público, cuando: (Incluido por Ley No. 13.964, 2019)
I - la prueba no puede realizarse por otros medios disponibles e igualmente efectivos; y (Incluido por la Ley N ° 13.964, de 2019)
II - existan elementos probatorios razonables de autoría y participación en infracciones penales cuyas penas máximas sean superiores a 4 (cuatro) años o en infracciones penales conexas. (Incluido por la Ley N ° 13.964, de 2019).
§ 1 La solicitud debe describir en detalle la ubicación y forma de instalación del dispositivo de captura ambiental. (Incluido por la Ley N ° 13.964, de 2019)
§ 2 (VETO).
§ 3º - La financiación ambiental no podrá exceder el plazo de 15 (quince) días, renovable por decisión judicial por períodos iguales, si se acredita la indispensabilidad de la prueba y cuando se presenta actividad delictiva permanente, habitual o continuada.
Como se desprende de la disposición legal, se requiere autorización judicial.

¿Es necesario autorización judicial para colocar una baliza en su país? ¿Hay regulada la posibilidad de utilizar judicialmente otras herramientas de geolocalización? En caso afirmativo, explique brevemente los requisitos exigibles.

En los delitos graves, la policía o fiscalía pueden captar la comunicación oral. Puede hacerlo la policía o la fiscalía mediando orden judicial, todo lo anterior de conformidad con el articulo 8-A de la ley 9.296 de 1996.

Para el caso de la colocación de balizas no existe regulación expresa, pero se podría realizar con orden judicial. La geolocalización a través de requisición de datos personales a empresas de telefonía móvil, rastreo de vehículos, o a través de pulseras de monitoreo electrónica de apenados, se puede realizar, siempre por orden del juez.

¿Qué obstáculos se encuentran cuando la autoridad judicial de su país ha de acceder a los datos de un proveedor de servicios que está situado en otro Estado?

Se permite solicitar los datos a la agencia del proveedor de internet en Brasil. Pero si hace falta una rogatoria, el procedimiento es difícil y requiere mucho tiempo.

¿Qué valor se otorga en su país a la prueba digital (e-evidence) obtenida por Comisión Rogatoria Internacional?

Vale como prueba y se tiene por legitima. La ley acerca de la cadena de custodia no trata de datos digitales, pero se aplican los procedimientos estándares internacionales.

En su país, ¿es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional?

Sí, pero hay casos en que el proveedor se niega a colaborar. Cuando es así se pueden imponer multas y otras medidas.

¿Considera adecuada la legislación de su país sobre obligación de conservación de datos por las operadoras de comunicación para la investigación y prueba de los delitos?

Se conservan los registros de conexión por 1 año y los registros de acceso a aplicaciones de internet por 6 meses (arts. 13 e 15 del Marco Civil de Internet).

El fiscal o el juez pueden librar ordenes de conservación por plazo más largo.

¿Tipifica su país bajo un título, capítulo, los ciberdelitos?

No informa.

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

No informa.

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

No informa.

¿Tiene su legislación procesal penal medidas restrictivas de internet (bloqueo, retiro de páginas web, etc.) en materia de ciberdelincuencia económica e intrusiva?

No informa.

¿Quiénes pueden solicitar y decretar estas medidas?

Son solicitados por el fiscal.

¿Existe en su país una normativa que regula específicamente las medidas de investigación tecnológica restrictivas de derechos fundamentales y cómo la valora?

No existe. Lo que se utiliza es la normativa vigente, tratando de adecuarla a los requerimientos, toda vez que, que se utiliza y pondera por el juez, caso a caso.

¿Cuáles son las medidas concretas de investigación con medios tecnológicos que contempla la legislación penal de su país?

Bajo el paraguas de las actuaciones de investigación en Chile, los fiscales que dirigen la investigación en forma exclusiva pueden encomendar a la policía diligencias de investigación que estimen conducentes para la misma. Deben registrar todo lo realizado, entregando al fiscal, también la posibilidad de pedir al juez de garantías la interceptación y grabación de las comunicaciones telefónicas o de otras formas de comunicación, siempre que existan sospechas fundadas y bajo un hecho determinado, el sentido que sirvan para dichos fines. Entre el abogado y el imputado, no se puede, a menos que el juez, lo estime por resolución que debe ser fundada. Todo lo anterior por 60 días prorrogables.

Es dable hacer presente que, cuando se pide abrir un teléfono celular por ejemplo, se ha utilizado la fórmula de la orden judicial de la entrada y registro de lugar cerrados, siempre y cuando existan antecedentes calificados para ello, Ley N° 19.223 del año 1993, que regula las figuras penales relacionadas con la informática, no contempla nada relacionado con la investigación, utilizándose en el Código Procesal Penal al efecto.

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

No informa.

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización judicial? ¿Cuál? y ¿Por qué no la exige?

No informa.

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

No informa.

¿Es necesario autorización judicial para colocar una baliza en su país? ¿Hay regulada la posibilidad de utilizar judicialmente otras herramientas de geolocalización? En caso afirmativo, explique brevemente los requisitos exigibles.

No informa.

¿Cómo valora la normativa interna de su país relativa a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos (celulares, tablets, computadoras...)?

No informa.

¿Qué obstáculos se encuentran cuando la autoridad judicial de su país ha de acceder a los datos de un proveedor de servicios que está situado en otro Estado?

No informa.

¿Qué valor se otorga en su país a la prueba digital (e-evidence) obtenida por Comisión Rogatoria Internacional?

No informa.

En su país, ¿es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional?

No informa.

¿Considera adecuada la legislación de su país sobre obligación de conservación de datos por las operadoras de comunicación para la investigación y prueba de los delitos?

Es adecuada, en Chile los proveedores tienen la obligación de conservar por 2 años, los datos, y antes era sólo 1 y se aumentó.

¿Tipifica su país bajo un título, capítulo, los ciberdelitos?

En Colombia existe un título que contempla los ciberdelitos en la Ley 599 del 2000, denominado "De la Protección de la Información y de los Datos"

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

Dentro del marco de la Ley 1273 del 5 de enero del 2009 se citan varios delitos de los cuales el contexto del verbo rector es invasivo o intrusivos; estos delitos son:

Artículo 269a. Acceso abusivo a un sistema informático.
Artículo 269b. Obstaculización ilegítima de sistema informático o red de telecomunicación
Artículo 269c. Interceptación de datos informáticos.
Artículo 269d. Daño informático.
Artículo 269e. Uso de software malicioso.
Artículo 269g. Suplantación de sitios web para capturar datos personales.

Así mismo, el delito de Pornografía con personas menores de 18 años, artículo 218, ley 599 del 2000.

¿Tiene su legislación procesal penal medidas restrictivas de internet (bloqueo, retiro de páginas web, etc.) en materia de ciberdelincuencia económica e intrusiva?

Estos bloqueos no están directamente establecidos dentro del Código Penal o del Código de Procedimiento Penal, pero si se han creado algunas leyes y normativas de prevención del delito que permite solicitar a los administradores de ISP en Colombia el bloqueo de direcciones IP de páginas web, con el fin de que no se permita su visualización en Colombia, gran parte de estas son páginas que pudieran ser empleadas como mecanismo tecnológico para la inducción y divulgación de la pornografía infantil, y otras páginas por temas tributarios como lo son las páginas de apuestas en línea internacionales.

Así mismo, el bloqueo puede ser realizado de manera administrativa una vez se compruebe la existencia de contenido ilícito, y también existen solicitudes expresas bien sea por parte de un juez de la república y también por un fiscal de conocimiento.

¿Cuáles son las medidas concretas de investigación con medios tecnológicos que contempla la legislación penal de su país?

Con respecto a esta pregunta las medidas tecnológicas existentes en Colombia están reguladas en la Ley 906 del 2004 y a pesar de que todas están reguladas dentro de las que se contemplan que no requieren autorización judicial, la búsqueda selectiva en base de datos si requiere autorización del Juez de Control de Garantías, no así la Interceptación de comunicaciones (art. 235), recuperación de información producto de la transmisión de datos a través de redes de comunicación (art. 236). La actuación de agente encubierto art. 242, cuando se hace de manera virtual las puede solicitar el Fiscal y las autoriza el juez de Control de Garantías.

¿Quiénes pueden solicitar y decretar estas medidas?

Algunas actividades son solicitadas por la Fiscalía General de la Nación ante un juez de control de garantías como las búsquedas selectivas en bases de datos y los registros CDR; otras actividades son realizadas como actos urgentes en la recaudación de información de la noticia criminal.

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

El derecho a la intimidad, el buen nombre.

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización judicial? ¿Cuál? y ¿Por qué no la exige?

No existe una medida de tal naturaleza.

¿Cómo valora la normativa interna de su país relativa a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos (celulares, tablets, computadoras...)?

De manera general podemos considerar que la normatividad procesal penal vigente les otorga un alto valor a estos medios de prueba e información legalmente recogidos, sin que se contemple algún condicionamiento que le reste poder suasorio al mismo en el marco de cualquier investigación penal.

¿Pueden los particulares y detectives o investigadores privados utilizar medidas tecnológicas de investigación sin autorización judicial y en qué supuestos?

Para obtener información que no requiera control previo si lo pueden realizar, aquellas actividades que requieres una orden de fiscal o de juez no.

¿Existe en su país una normativa que regula específicamente las medidas de investigación tecnológica restrictivas de derechos fundamentales y cómo la valora?

En materia normativa vale la pena resaltar lo conceptuado por la Corte Constitucional en la sentenciaC-336/07. Concretamente para el tópico relacionado con el acto de investigación de búsqueda selectiva de información confidencial requiere autorización previa del juez de control de garantías; consulta selectiva de información que se acopia con fines legales, por instituciones o entidades públicas o privadas debidamente autorizadas para ello.

Así mismo, las consideraciones que sobre el particular expresan en torno a la vulneración en la facultad para acceder a información confidencial sin autorización judicial previa y la necesidad de control previo por juez de control de garantías para estas medidas.

Finalmente, en torno al derecho del habeas data, las reflexiones que giran en torno al método investigativo sobre búsqueda se-

lectiva de información confidencial del indiciado o imputado y los presupuestos que deben ser objeto de estudio por parte del juez de control de garantías, para autorizar búsqueda selectiva de información confidencial del indiciado o imputado en bases de datos.

¿Qué valor se otorga en su país a la prueba digital (e-evidence) obtenida por Comisión Rogatoria Internacional?

Una vez obtenida siempre que se encuentre dentro de los términos legales para su posterior legalización ante un juez de control de garantías es viable y aceptada.

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

Sobre este asunto, lo más cercano tiene ocurrencia con la utilización del agente encubierto amparado dentro del Código de Procedimiento Penal. Este opera cuando el fiscal tiene motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este Código, para inferir que el indiciado o el imputado en la investigación que se adelanta, continúa desarrollando una actividad criminal.

Para iniciar con esta técnica investigativa es necesario previa autorización del Director Nacional o Seccional de Fiscalías, quien podrá ordenar la utilización de agentes encubiertos, siempre que resulte indispensable para el éxito de las tareas investigativas.

En desarrollo de esta facultad especial podrá disponerse que uno o varios funcionarios de la policía judicial o, incluso particulares, quienes puedan actuar en esta condición y realizar actos extrapenales con trascendencia jurídica. En consecuencia, dichos agentes estarán facultados para intervenir en el tráfico comercial, asumir obligaciones, ingresar y participar en reuniones en el lugar de trabajo o domicilio del indiciado o imputado y, si fuere necesario, adelantar transacciones con él. Igualmente, si el agente encubierto encuentra que en los lugares donde ha actuado existe información útil para los fines de la investigación, lo hará saber al fiscal para que este disponga el desarrollo de una operación especial, por parte de la policía judicial, con miras a que se recoja la información y los elementos materiales probatorios y evidencia física hallados.

Así mismo, podrá disponerse que actúe como agente encubierto el particular que, sin modificar su identidad, sea de la confianza del indiciado o imputado o la adquiera para los efectos de la búsqueda y obtención de información relevante y de elementos materiales probatorios y evidencia física.

Durante la realización de los procedimientos encubiertos podrán utilizarse los medios técnicos de ayuda previstos en el artículo 239.

¿Es necesario autorización judicial para colocar una baliza en su país? ¿Hay regulada la posibilidad de utilizar judicialmente otras herramientas de geolocalización? En caso afirmativo, explique brevemente los requisitos exigibles.

Si es preciso orden judicial previa. En el Código de Procedimiento Penal se encuentra el artículo 239.

Sin perjuicio de los procedimientos preventivos que adelanta la fuerza pública en cumplimiento de su deber constitucional, el fiscal que tuviere motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este Código para inferir que el indiciado o el imputado pudiere conducirlo a conseguir información útil para la investigación que se adelanta, podrá disponer que se someta a seguimiento pasivo, por tiempo determinado, por parte de la Policía Judicial. Si en el lapso de un (1) año no se obtuviere resultado alguno, se cancelará la orden de vigilancia, sin perjuicio de que vuelva a expedirse, si surgieren nuevos motivos. En la ejecución de la vigilancia se empleará cualquier medio que la técnica aconseje.

En consecuencia, se podrán tomar fotografías, filmar videos y, en general, realizar todas las actividades relacionadas que permitan recaudar información relevante a fin de identificar o individualizar los autores o partícipes, las personas que lo frecuentan, los lugares a donde asiste y aspectos similares, cuidando de no afectar la expectativa razonable de la intimidad del indiciado o imputado o de terceros.

En todo caso se surtirá la autorización del Juez de Control de Garantías para la determinación de su legalidad formal y material, dentro de las treinta y seis (36) horas siguientes a la expedición de la orden por parte de la Fiscalía General. Vencido el término de la orden de vigilancia u obtenida la información útil para la investigación el fiscal comparecerá ante el Juez de Control de Garantías, para que realice la audiencia de revisión de legalidad sobre lo actuado.

¿Qué obstáculos se encuentran cuando la autoridad judicial de su país ha de acceder a los datos de un proveedor de servicios que está situado en otro Estado?

En lo que atañe a las facultades para tener acceso a datos de proveedores extranjeros es necesario indicar que las autoridades judiciales colombianas cuentan con el apoyo de las empresas más relevantes en Estados Unidos, tales como: Whatsapp; Facebook; Google; Twitter; Hotmail; Yahoo; Gmail; Youtube; Instagram; Amazon; Apple; Microsoft; Skype; Github; Dropbox; eBay; Paypal; Netflix; Uber; Oracle. Pues existen canales aportados por ellos mismos para solicitar información mediante búsqueda selectiva en bases de datos

En su país, ¿es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional?

Las autoridades judiciales responsables de la persecución del delito cuentan con las facultades para acudir directamente a la fuente de información para recolectarla y posteriormente legalizar los hallazgos ante los jueces de control de garantía.

¿Considera adecuada la legislación de su país sobre obligación de conservación de datos por las operadoras de comunicación para la investigación y prueba de los delitos?

Actualmente se cuentan con varios mecanismos de apoyo entre las empresas privadas y públicas para preservar y aportar oportunamente la información.

¿Tipifica su país bajo un título, capítulo, los ciberdelitos?

No informa.

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

La legislación penal de Costa Rica contempla las siguientes figuras típicas relacionadas con ciberdelincuencia económica: Estafa Informática 217 bis. Sabotaje Informático 229 ter. Espionaje Informático 231. Instalación o Propagación de Programas Informático Maliciosos 232.

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

La legislación penal de Costa Rica contempla las siguientes figuras típicas relacionadas con ciberdelincuencia intrusiva: Daño Informático 229 bis, Suplantación de Identidad 230, Suplantación de Páginas Electrónicas 233, Facilitación de Delito Informático 234, Difusión de Información Falsa 236, Coacción 193, Amenazas Agravadas 195, Violación de Secretos 196, Violación de Datos Personales, Sustracción, Desvío o Supresión de Correspondencia 197, Captación Indebida de Manifestaciones Verbales 198, Uso Indebido de Correspondencia 201, Propalación 202, Divulgación de Secretos 203, Extorsión 214, Apoyo y Servicio para el Terrorismo 281 bis, Intimidación Pública 282, Apología del Delito 283, Menosprecio de los Símbolos de una Nación Extranjera 292, Revelación de Secreto de Estado 293, Revelación por Culpa 294, Espionaje 295, Intrusión 296, Daño en Objeto de Interés Militar 300, Propaganda Contra el Orden Constitucional 303, Motín 304, Menosprecio para los Símbolos Nacionales 305, Conspiración 307, Atentado 311, Desobediencia 314, Molestia o Estorbo a la Autoridad 315, Amenaza a un Funcionario Público 316, Favorecimiento Real 332, Divulgación de Información Confidencial 332 bis, Injurias 145, Difamación 146, Calumnia 147, Ofensa a la Memoria de un Difunto 148, Publicación de Ofensas 152, Difamación de una Persona Jurídica 153, Actos Sexuales Remunerados con Persona Menor de Edad 160, Turismo Sexual 162 bis, Corrupción 167, Seducción o Encuentros con Menores por Medios Electrónicos 167 bis, Corrupción Agravada 168, Proxenetismo 169, Proxenetismo Agravado 170, Fabricación, Producción o Reproducción de Pornografía 173, Tenencia de Material Pornográfico 173 bis, Difusión de Pornografía 174, Pornografía Virtual y Pseudo Pornografía 174 bis, Delitos propios de la Ley de Propiedad Intelectual, Amenazas contra una Mujer e Incumplimiento de una Medida de Protección de la Ley de Penalización de Violencia contra la Mujer.

¿Tiene su legislación procesal penal medidas restrictivas de internet (bloqueo, retiro de páginas web, etc.) en materia de ciberdelincuencia económica e intrusiva?

En Costa Rica, ni el código de rito ni tampoco la ley penal sustantiva poseen mecanismos procesales concretos para gestionar medidas restrictivas en casos de delitos cometidos por medio de redes o internet, se debe de hacer uso del Convenio de Budapest, y la solicitud para preservación de información puede hacerla tanto la Policía Judicial, el Ministerio Público o bien el juez, mientras que en caso de que se requiera una medida cautelar más sólida tendiente a bloquear información que eventualmente se encuentre en el exterior, debe de gestionarse con control jurisdiccional.

Por otra parte, en la práctica ante publicaciones en páginas nacionales normalmente basta con la solicitud que realice la Policía Judicial para que las personas que manejan las páginas accedan a hacerlo, ello siempre y cuando no conformen parte de la eventual estructura que comete el delito, por otra parte existe una figura administrativa que es MICITT (Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones) adscrito al poder ejecutivo, el cual rastrea y detecta páginas y publicaciones maliciosas y procede al bloqueo de las mismas

¿Cuáles son las medidas concretas de investigación con medios tecnológicos que contempla la legislación penal de su país?

Actualmente en Costa Rica la normativa procesal penal no contempla formalmente en código de rito, procedimiento de investigación que regulen investigaciones mediante medidas tecnológicas, no obstante en virtud de que nos rigen principios tales como los de objetividad, legalidad y libertad probatoria, regulada en los artículos 180, 181 y 182, es viable hacer uso de cualquier medio probatorio. Por otra parte, en donde podría indicarse que existe regulación escueta y que se utiliza para la recopilación de este tipo de elementos probatorios tecnológicas es la Ley Sobre el Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones o Ley Número 7425 del 09 de agosto de 1994, como se observa es una ley ya de prácticamente 30 años, a mi criterio desactualizada, puesto que en la práctica de debemos de hacer uso de ella en relación a tecnología que evidentemente en aquella época no existía.

De dicho cuerpo normativo se hace uso para gestionar la autorización de decomiso de evidencia digital que proviene de diligencias de allanamiento, su posterior respaldo y análisis, así como para el tema de las intervenciones telefónicas.

¿Quiénes pueden solicitar y decretar estas medidas?

Las relacionadas a la ley antes indicada y de acuerdo al artículo 24 de la Constitución Política de Costa Rica, para los casos concretos, deben de ser ordenadas por parte del órgano jurisdiccional, propiamente el de etapa de investigación (que es un juez de garantías, siendo el mismo que labora en la siguiente etapa intermedia), esto previa solicitud del representante del Ministerio Público, de la Policía Judicial o de cualquiera de las partes, existe la particularidad que la solicitud de intervención de las comunicaciones (de cualquier tipo incluidas las digitales) solo aplicará en los delitos de secuestro extorsivo, corrupción agravada, proxenetismo agravado, fabricación o producción de pornografía, tráfico de personas y tráfico de personas para comercializar sus órganos, homicidio calificado, genocidio, terrorismo y los delitos previstos en la ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, legitimación de capitales y actividades conexas, y se presenta la tesis que solo puede requerirla formalmente el Fiscal General de la República o el Director del Organismo de Investigación Judicial, de conformidad al artículo 10, así como cualquier parte del proceso, no obstante existe jurisprudencia que contrapone dicha posición y permite que lo sea el Fiscal que instruye la causa.

Igualmente, con respecto al tema de la información telefónica relacionada al estudio de llamadas entrantes y salientes, flujogramas o localización mediante estudio de activación de radio bases, no existe recelo y bien puede ser gestionado por parte de la policía judicial o el ente fiscal sin mayor problema.

¿Pueden los particulares y detectives o investigadores privados utilizar medidas tecnológicas de investigación sin autorización judicial y en qué supuestos?

Es factible que las partes, o bien los investigadores, aporten elementos de prueba tecnológica (videos, fotografías, enlaces, capturas, grabaciones, etc), siempre y cuando las mismas no requieran el control de la Ley Sobre el Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones, básicamente si no violentan la privacidad y si fueron recopiladas mediante medios lícitos, la descripción de los documentos privados que requieren control judicial están previsto en el artículo 1 de dicho cuerpo normativo, y lo son: la correspondencia epistolar, por fax, télex, telemática o cualquier otro medio; los videos, los casetes, las cintas magnetofónicas, los discos, los disquetes, los escritos, los libros, los memoriales, los registros, los planos, los dibujos, los cuadros, las radiografías, las fotografías y cualquier otra forma de registrar información de carácter privado, utilizados con carácter representativo o declarativo, para ilustrar o comprobar algo. Mientras que las comunicaciones son reguladas en el numeral 9, y son las: orales, escritas o de otro tipo, incluso las telecomunicaciones fijas, móviles, inalámbricas y digitales.

¿Existe en su país una normativa que regula específicamente las medidas de investigación tecnológica restrictivas de derechos fundamentales y cómo la valora?

No existe en Costa Rica, normativa específica que regule las medidas de investigación tecnológica que eventualmente sea restrictiva de derechos fundamentales, la única norma que podría encajar en dicha categoría, en donde se afecta un derecho fundamental, como lo sería el derecho a la comunicación, lo sería el artículo 261 del Código Procesal Penal, el cual regula la incomunicación del imputado, de lo cual podrá hacerlo el ente Fiscal o la policía por el plazo máximo de 6 horas para luego requerir ante el juez la respectiva orden formal, la cual debe de ser fundada y hasta por el plazo máximo de 10 días consecutivos, y se requiere que de previo si dicte prisión preventiva (en caso de que sea viable), y tiene como fin el impedir que el investigado se comunique con sus eventuales cómplices u obstaculice la investigación, sin embargo no impedirá que éste se comunique con su defensa técnica.

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

El ordenamiento jurídico costarricense y la puesta en práctica de dichas normas en su realidad jurídica es sumamente garantista, de tal forma la actuación del juez de garantías a la hora de analizar la posibilidad de aplicación de una medida tecnológica para recopilación de prueba o bien para la admisión de dicha prueba (así como de cualquier otra), se regulan en el artículo 183 y siguientes del Código Procesal Penal, siempre regirá la legalidad, pero además se tomarán en cuenta principios como el de utilidad, e identidad de la prueba respecto a lo que pretende probar.

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

No existe en Costa Rica, regulación formal respecto a la utilización de micrófonos para investigaciones penales, buscando jurisprudencia no denoto que se haya utilizado dicho medio de prueba alguna vez, de igual forma en mis 11 años de carrera judicial tampoco recuerdo que en alguna oportunidad se utilizara tal situación, no obstante pese a dicho vacío normativo, en caso de que lo que se pretende obtener sea información de comunicaciones, debería de seguirse el procedimiento para la intervención telefónica, puesto que lo contrario sería una captación ilícita de comunicaciones, delito el cual regula la propia normal especial en su artículo 24 con pena de prisión de 1 a 3 años.

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización judicial? ¿Cuál? y ¿Por qué no la exige?

Dentro de esa libertad probatoria algunas diligencias tendientes a recopilar prueba tecnológica podrían ser: como se indicó el estudio de llamadas, análisis de activación de radios bases, requerir y obtener información de operadores de servicio sobre datos de usuario, datos de tráfico, verificación de grabaciones en sitios públicos, estudio de perfil de investigado en redes sociales, consultas en otras fuentes abiertas, obtención de prueba mediante el consentimiento del derecho habiente, etc.

Estás medidas antes indicadas, no requieren control jurisdiccional, por cuanto se encuentran fuera de la esfera de regulación de la única ley especial (ya analizada) que da custodia al bien jurídica privacidad, en el curso de una investigación penal.

¿Es necesario autorización judicial para colocar una baliza en su país? ¿Hay regulada la posibilidad de utilizar judicialmente otras herramientas de geolocalización? En caso afirmativo, explique brevemente los requisitos exigibles.

De igual en cuanto a la colocación de dispositivos de ubicación o mediante GPS, no existe regulación alguna, y no se requiere autorización judicial, de hecho es una práctica poco frecuente, y al ser Costa Rica un país tan pequeño, lo más frecuente es que se realicen seguimiento o vigilancias policiales para casos específicos en donde se pretende ubicar o dar seguimiento a un investigado, así como el conocer sus movimientos y contactos habituales.

¿Cómo valora la normativa interna de su país relativa a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos (celulares, tablets, computadoras...)?

Respecto a este tema en Costa Rica, deben de diferenciarse diferentes estadios, el primero de ellos que es la custodia de la evidencia, ello ha sido ampliamente discutido, existe basta jurisprudencias, así mismo los funcionarios recibimos amplías capacitaciones respecto al adecuado manejo de cadena de custodia, aunado a ello la Defensa Pública (quienes en su mayoría atienden los asuntos penales) son sumamente celosos y contralores de ese adecuado manejo, de tal suerte creo que modestia aparte dicho tema ya se encuentra debidamente superado en el país, ahora bien en cuanto a la obtención de la evidencia digital, actualmente junto a otro compañero, me encuentro

desarrollando un ensayo al respecto, y es que existe una falta de familiaridad o temor hacia lo novedoso, hacia lo tecnológico, lo cual sumado a lo garantista del proceso penal costarricense, se hacen uso de prácticas no regladas, que buscan aún más proteger ese velo de una sana y adecuada obtención de la prueba, lo cual torna en odioso y complicado en relación a los plazos, el tema del acceso y obtención de dicho tipo de prueba digital.

A modo de ejemplo, luego de decomisado un teléfono celular, se debe de requerir al juez que permita el acceso a dicho dispositivo para recopilar de manera probable determinada prueba, una vez autorizado se debe de dejar en manos de la Sección Contra el Cibercrimen del Organismo de Investigación Judicial, la cual es la única oficina centralizada en la capital del país que realiza dicha diligencia, y posteriormente se convoca a audiencia a todas las partes, para que presencien la diligencia.

Lo anterior provoca es que la agenda de la sección antes indicada, se encuentre saturada ya que debido a esta mala práctica, que como indicó, no se encuentra normada, los obliga a viajar por todo el territorio nacional compareciendo a realizar dichas extracciones en audiencias conocidas como de "apertura de evidencia electrónica", esta mala práctica consuetudinaria, no posee razón de ser, puesto que en dicha diligencia que es propia de una pericia (pese a que en Costa Rica no esté así regulada, ni se cuente con las certificaciones al respecto, diferente a todas las demás que ofrece el amplío Complejo Forense), se apersone las partes prácticamente a estorbar, ya que los abogados no tenemos el conocimiento técnico de lo que ahí se realiza, parte de los que se está buscando, es que se unifiquen criterios en las fiscalías del país, mediante una herramienta que exponga todos estos problemas, y que se equipara dicha diligencia a una pericia como tal, para luego únicamente poner en conocimiento de las partes el resultado de la misma. Esto evidentemente llevará tiempo, pero dichosamente ya existimos dos personas interesadas en romper este paradigma y en buscar formas más efectivas y eficientes de manejar las investigaciones y de enfocar el recurso institucional.

¿Qué obstáculos se encuentran cuando la autoridad judicial de su país ha de acceder a los datos de un proveedor de servicios que está situado en otro Estado?

De manera general se comparte la percepción de que en esta materia siempre existe problema por los prolongados tiempos de espera o las nulas respuestas frente a lo peticionado, lo engorroso del trámite, y las dificultades naturales de las fronteras culturales representada en los idiomas o las diferencias horarias.

En su país, ¿es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional?

Con la creación de la Unidad de Cibercrimen de la Fiscalía Adjunta de Fraudes y Cibercrimen de San José, al ser la única fiscalía especializada en el país en relación a dicha materia, se ha asumido el reto de tomar posiciones innovadoras para la solución de los problemas intrínsecos de la practica judicial para la persecución de la cibercriminalidad.

En ese marco de esfuerzos conjunto se ha logrado generar contacto con proveedores de servicio internacionales, mediante medios expeditos como lo son correos electrónicos, haciendo para ello mención de las facilidades normadas de acuerdo al Convenio de Budapest, ello con excelentes resultados.

No obstante lo anterior, es bien sabido que hay otras empresas (las mismas que presentan dificultades para la colaboración judicial a nivel prácticamente mundial) de las cuales no obtenemos si quiera una respuesta monosilábica. Ello nos impulsa por responsabilidad y objetividad en nuestras funciones que debamos adelantar el tedioso procedimiento legal, para muchas veces de nuevo no obtener respuesta o en el mejor de los casos una respuesta negativa a nuestra gestión.

¿Qué valor se otorga en su país a la prueba digital (e-evidence) obtenida por Comisión Rogatoria Internacional?

En Costa Rica, partiendo del supuesto de que se otorgue una adecuada respuesta a un trámite de Carta Rogatoria, en donde se obtenga evidencia digital internacional, en caso de que la misma fuese recopilada por medios lícitos, y después de analizada por las partes, se le debe de dar el mismo valor probatorio que a la prueba recopilada en territorio nacional.

¿Considera adecuada la legislación de su país sobre obligación de conservación de datos por las operadoras de comunicación para la investigación y prueba de los delitos?

Nuevamente este aspecto es débil en la realidad nacional, las regulaciones para que las operadoras de comunicación brinden información para las investigaciones penales nacen de acuerdos institucionales y controles de índole administrativo, mas no judiciales o legales. En consecuencia existe una plataforma llamada Sistema Informático de Solicitudes de Telecomunicaciones, conformado por las empresas de telecomunicaciones que operan en el país, y al cual tienen acceso las jefaturas del Ministerio Público y de la Policías Judicial, quienes pueden requerir información por dicho medio, sin control jurisdiccional, no obstante en la práctica, generalmente se obtiene información para el caso de parte de la operadora gubernamental, y no de las operadoras privadas, así mismo los plazos de respuesta son largos.

¿Tipifica su país bajo un título, capítulo, los ciberdelitos?

La legislación penal cubana no contempla ningún título y tampoco ningún capítulo destinado a los ciberdelitos. Para el país participante la temática es nueva por lo cual, desde lo sustantivo y procesal no poseen tipificación, así como tampoco medios tecnológicos investigativos.

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

No informa.

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

No informa.

¿Tiene su legislación procesal penal medidas restrictivas de internet (bloqueo, retiro de páginas web, etc.) en materia de ciberdelincuencia económica e intrusiva?

No informa.

¿Cuáles son las medidas concretas de investigación con medios tecnológicos que contempla la legislación penal de su país?

No informa.

¿Quiénes pueden solicitar y decretar estas medidas?

No informa.

¿Pueden los particulares y detectives o investigadores privados utilizar medidas tecnológicas de investigación sin autorización judicial y en qué supuestos?

No informa.

¿Existe en su país una normativa que regula específicamente las medidas de investigación tecnológica restrictivas de derechos fundamentales y cómo la valora?

No informa.

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

No informa.

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización judicial? ¿Cuál? y ¿Por qué no la exige?

No informa.

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

No informa.

¿Es necesario autorización judicial para colocar una baliza en su país? ¿Hay regulada la posibilidad de utilizar judicialmente otras herramientas de geolocalización? En caso afirmativo, explique brevemente los requisitos exigibles.

No informa.

¿Cómo valora la normativa interna de su país relativa a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos (celulares, tablets, computadoras...)?

No informa.

En su país, ¿es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional?

No informa.

¿Qué obstáculos se encuentran cuando la autoridad judicial de su país ha de acceder a los datos de un proveedor de servicios que está situado en otro Estado?

No informa.

¿Qué valor se otorga en su país a la prueba digital (e-evidence) obtenida por Comisión Rogatoria Internacional?

No informa.

¿Considera adecuada la legislación de su país sobre obligación de conservación de datos por las operadoras de comunicación para la investigación y prueba de los delitos?

No informa.

¿Tipifica su país bajo un título, capítulo, los ciberdelitos?

A distinción de muchos países que integran su normativa sustantiva penal en un solo cuerpo legal denominado Código Penal, el Ecuador ha promulgado una normativa que recoge el derecho penal sustantivo, adjetivo y ejecutivo en III libros unificados por un solo cuerpo legal llamado Código Orgánico Integral Penal.

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

Dentro del catálogo de delitos que contempla a legislación penal ecuatoriana se encuentran los siguientes tipos penales que pueden tener conexión directa con la ciberdelincuencia económica, siendo éstos los siguientes: Art. 186.- Estafa, empleando medios electrónicos; Art. 190.- Apropiación fraudulenta por medios electrónicos; Art. 191.- Reprogramación o modificación de información de equipos terminales móviles; Art. 192.- Intercambio, comercialización o compra de información de equipos terminales móviles; Art. 193.- Reemplazo de identificación de terminales móviles; Art. 194.- Comercialización ilícita de terminales móviles; Art. 195.- Infraestructura ilícita; Art. 230.- Interceptación ilegal de datos; Art. 231.- Transferencia electrónica de activo patrimonial; Art. 232.- Ataque a la integridad de sistemas informáticos; Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

Art. 103.- Pornografía con utilización de niñas, niños o adolescentes.; Art. 154.1.- Instigación al suicidio; Art. 173.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos; Art. 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos; Art. 178.- Violación a la intimidad; Art. 211.- Supresión, alteración o suposición de la identidad y estado civil.; Art. 229.- Revelación ilegal de base de datos.

¿Tiene su legislación procesal penal medidas restrictivas de internet (bloqueo, retiro de páginas web, etc.) en materia de ciberdelincuencia económica e intrusiva?

El Código Orgánico Integral Penal contempla las siguientes técnicas de investigación: Operaciones encubiertas (Art. 483), entregas vigiladas o controladas (Art. 485), la cooperación eficaz (Art. 491), investigaciones conjuntas y asistencia judicial recíproca (Arts. 496 y 497).

¿Cuáles son las medidas concretas de investigación con medios tecnológicos que contempla la legislación penal de su país?

No existe en el Código Orgánico Integral Penal ecuatoriano.

¿Quiénes pueden solicitar y decretar estas medidas?

Las técnicas de investigación son dirigidas por la unidad especializada de la Fiscalía. Podrá solicitarse por el personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, entregando a la o al fiscal los antecedentes necesarios que la justifiquen. Por lo tanto, quien la solicita es el Fiscal.

La autorización la concede el juez de garantías penales, la cual debe ser debidamente fundamentada y responder al principio de necesidad para la investigación, se deberá imponer limitaciones de tiempo y controles que sean de utilidad para un adecuado respeto a los derechos de las personas investigadas o procesadas.

¿Pueden los particulares y detectives o investigadores privados utilizar medidas tecnológicas de investigación sin autorización judicial y en qué supuestos?

No informa

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

No informa

¿Existe en su país una normativa que regula específicamente las medidas de investigación tecnológica restrictivas de derechos fundamentales y cómo la valora?

El Art. 5 del Código Orgánico Integral Penal recoge los principios procesales, del derecho al debido proceso penal, sin perjuicio de otros establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado.

De acuerdo al Art. 459.3 del mismo cuerpo de leyes, las diligencias de investigación deberán ser registradas en medios tecnológicos y documentales más adecuados para preservar la realización de la misma y formarán parte del expediente fiscal.

De su parte, el Art. 476 dispone que el juzgador ordenará la interceptación de las comunicaciones o datos informáticos, previa solicitud fundamentada del fiscal, cuando existan indicios que resulten relevantes a los fines de la investigación.

Conforme al Art. 454.1 ibidem, las investigaciones y pericias practicadas durante la investigación alcanzarán el valor de prueba, una vez que sean presentadas, incorporadas y valoradas en la audiencia oral de juicio.

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización judicial? ¿Cuál? y ¿Por qué no la exige?

No informa

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

No informa

¿Es necesario autorización judicial para colocar una baliza en su país? ¿Hay regulada la posibilidad de utilizar judicialmente otras herramientas de geolocalización? En caso afirmativo, explique brevemente los requisitos exigibles.

No informa

¿Cómo valora la normativa interna de su país relativa a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos (celulares, tablets, computadoras...)?

No informa

¿Qué obstáculos se encuentran cuando la autoridad judicial de su país ha de acceder a los datos de un proveedor de servicios que está situado en otro Estado?

No informa

¿Qué valor se otorga en su país a la prueba digital (e-evidence) obtenida por Comisión Rogatoria Internacional?

No informa

En su país, ¿es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional?

No informa

¿Considera adecuada la legislación de su país sobre obligación de conservación de datos por las operadoras de comunicación para la investigación y prueba de los delitos?

La Ley Orgánica de Telecomunicaciones establece las regulaciones necesarias para garantizar la seguridad de las comunicaciones y la protección de datos personales. Los prestadores de servicios deberán proveer toda la información requerida en la orden de interceptación, incluso los datos de carácter personal de los involucrados en la comunicación, así como la información técnica necesaria y los procedimientos para la descomprensión, descifrado o decodificación en caso de que las comunicaciones objeto de la interceptación legal hayan estado sujetas a tales medidas de seguridad.

El problema radica en que, las operadoras no mantienen en forma permanente la información, (solo 30 días), para que la Fiscalía pueda investigar el cometimiento de una infracción.

¿Tipifica su país bajo un título, capítulo, los ciberdelitos?

Sobre el particular existe la Ley Especial Contra los Delitos Informáticos y Conexos, creada en el año 2016.

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

En materia de tipificación de delitos económicos cometidos a través de los medios electrónicos, internet o nuevas tecnologías es necesario acudir a la Ley Especial Contra los Delitos Informáticos y Conexos, la cual fue creada en febrero del 2016; la misma contiene los siguientes delitos cibereconómicos: Estafa Informática, Fraude Informático, Espionaje Informático, Hurto por Medios Informáticos, Técnicas de denegación de Servicio, 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 y Disponibilidad de los Datos, Daños a Sistema Informáticos, posesión de Equipo o Prestación de Servicios para la Vulneración de la Seguridad.

¿Tiene su legislación procesal penal medidas restrictivas de internet (bloqueo, retiro de páginas web, etc.) en materia de ciberdelincuencia económica e intrusiva?

Ni la Ley especial ni el Código Penal o Procesal penal de El Salvador contempla ninguna medida restrictiva de internet, para aquellos delitos informáticos.

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

De igual forma, en materia de ciberdelincuencia intrusiva es necesario acudir a la Ley Especial Contra los Delitos Informáticos y Conexos, el cual contiene los siguientes delitos: Pornografía a través del Uso de Tecnologías de Información y la Comunicación, utilización de Niñas, Niños, Adolescentes o Personas con Discapacidad en Pornografía a través del Uso de las Tecnologías de la Información y la Comunicación, Adquisición o Posesión de Material Pornográfico de Niñas, niños, Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación, Corrupción de Niñas, niños, Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación, Acoso de Niñas, niños, Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación, Condiciones Agravantes Comunes, Acoso a través de Tecnologías de la Información y la Comunicación, Revelación Indebida de datos o Información de Carácter Personal, Utilización de Datos Personales, obtención y Transferencia de Información de Carácter Confidencial, Divulgación No Autorizada, Hurto de Identidad, Interceptación de Transmisión entre Sistemas de las Tecnologías de la Información y la Comunicación, Interferencia de datos, Violación de la Seguridad del Sistema, Posesión de Equipos o Prestación de Servicios para la Vulneración de la Seguridad Acceso Indebido a Sistemas Informáticos, Interferencia del Sistema Informático.

¿Cuáles son las medidas concretas de investigación con medios tecnológicos que contempla la legislación penal de su país?

En el caso del Código Procesal Penal Salvadoreño solo existe un artículo que hace referencia a las medidas tecnológicas y este es el artículo 201, el cual establece:
Obtención y resguardo de información electrónica Art. 201.- Cuando se tengan razones fundadas para inferir que una persona posee información constitutiva de delito o útil para la investigación, almacenada en equipos o instrumentos tecnológicos de su propiedad o posesión, el fiscal solicitará la autorización judicial para adoptar las medidas que garanticen la obtención, resguardo o almacenamiento de la información; sin perjuicio que se ordene el secuestro respectivo.

¿Quiénes pueden solicitar y decretar estas medidas?

En este caso como lo establece el artículo 201 del Código Procesal Penal Salvadoreño, lo puede solicitar el ente Fiscal, y la autoridad que autoriza es el Juez de la causa.

¿Pueden los particulares y detectives o investigadores privados utilizar medidas tecnológicas de investigación sin autorización judicial y en qué supuestos?

No informa

¿Existe en su país una normativa que regula específicamente las medidas de investigación tecnológica restrictivas de derechos fundamentales y cómo la valora?

El Salvador cuenta con la Ley Especial para la Intervención de las Comunicaciones con vigencia desde marzo 2010, esto es derivado de reforma constitucional del art. 24, siendo una normativa que permite de manera excepcional la intervención temporal de comunicaciones con condiciones previas de intervención como lo es bajo control y autorización judicial, siendo competentes los jueces de instrucción con sede en San Salvador. Además, debe existir un procedimiento de investigación, no cabe intervención telefónica para tratar de descubrir indiscriminadamente delitos, es decir concedida la autorización no cabe que se investiguen delitos distintos, solo es un hecho delictivo, y se dice una vulneración vulnera el derecho fundamental de la intimidad y otros derechos cuando se produce una novación del tipo penal investigado, por lo que la autorización debe especificar cuál será el dispositivo o bien el número o números del teléfono sobre los que recae la investigación, pues en los casos de los teléfonos, si este es distinto del autorizado provoca la ineficacia probatoria.

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

No informa

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización judicial? ¿Cuál? y ¿Por qué no la exige?

No informa

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

No informa

¿Es necesario autorización judicial para colocar una baliza en su país? ¿Hay regulada la posibilidad de utilizar judicialmente otras herramientas de geolocalización? En caso afirmativo, explique brevemente los requisitos exigibles.

No informa

¿Cómo valora la normativa interna de su país relativa a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos (celulares, tablets, computadoras...)?

No informa

¿Qué obstáculos se encuentran cuando la autoridad judicial de su país ha de acceder a los datos de un proveedor de servicios que está situado en otro Estado?

No informa

¿Qué valor se otorga en su país a la prueba digital (e-evidence) obtenida por Comisión Rogatoria Internacional?

No informa

En su país, ¿es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional?

No informa

¿Considera adecuada la legislación de su país sobre obligación de conservación de datos por las operadoras de comunicación para la investigación y prueba de los delitos?

Se considera adecuada dicha normativa en tanto constituye una herramienta esencial en la lucha contra la criminalidad tradicional y sobre todo contra la criminalidad organizada o no convencional, garantizando el derecho humano de las personas a la comunicación.

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

Existe legislación especializada respecto a la prevención, control y sanción en actos de índole sexual, explotación y trata de personas (Decreto 9-2009 del Congreso de la República de Guatemala, que contiene la Ley contra la Violencia Sexual, Explotación y Trata de personas) en la cual se describen figuras penales tales como: producción de pornografía de personas menores de edad; comercialización o difusión de pornografía de personas menores de edad y la posesión de material pornográfico (arts. 40 y subsiguientes) que son concordantes con los artículos 194 y subsiguientes del Código Penal, solo que se sancionan con una pena mayor a los otros señalados en el párrafo anterior con pena de prisión que oscila entre 6 a 10 años. Por otra parte, también se sanciona con pena prisión y pena multa a quien creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas; en el mismo orden de ideas, se sanciona a quien manipule, oculte, altere o distorsione información requerida para actividad comercial, por ejemplo, quien altere, falsee estados contables o la situación patrimonial (arts. 274D y 274E).

¿Cuáles son las medidas concretas de investigación con medios tecnológicos que contempla la legislación penal de su país?

Guatemala cuenta con una normativa especializada, la Ley en contra la Delincuencia Organizada (Decreto 21-2006), en la cual se detalla no solo el compromiso asumido como país sino distintas definiciones acordes con esa normativa, las figuras delictivas que abarca para combatirlas, prevenirlas y sobre todo la cooperación internacional que es vital para erradicar este flagelo de la delincuencia organizada.

El ordenamiento adjetivo penal guatemalteco contempla las medidas de investigación básicas pero esta ley las desarrolla, se puede encontrar títulos completos que relacionan los métodos y medios especiales de investigación criminal. Si bien es cierto en mi caso, como jueza sentenciadora no otorgó ni autorizo este tipo de investigación ya que son propias de la etapa preparatoria e intermedia; pero durante la etapa de juicio si es de vital importancia que las mismas se otorguen cumpliéndose las formalidades y requisitos que la ley impone para llegar a tener éxito al momento de analizar los medios probatorios.

¿Tiene su legislación procesal penal medidas restrictivas de internet (bloqueo, retiro de páginas web, etc.) en materia de ciberdelincuencia económica e intrusiva?

No informa.

¿Quiénes pueden solicitar y decretar estas medidas?

Se indica que las puede solicitar el Ministerio Público, pero no indica quién es el funcionario encargado de decretarla

¿Pueden los particulares y detectives o investigadores privados utilizar medidas tecnológicas de investigación sin autorización judicial y en qué supuestos?

No informa

¿Existe en su país una normativa que regula específicamente las medidas de investigación tecnológica restrictivas de derechos fundamentales y cómo la valora?

Ley contra la Delincuencia Organizada

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

No informa

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización judicial? ¿Cuál? y ¿Por qué no la exige?

No informa

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

No informa

¿Es necesario autorización judicial para colocar una baliza en su país? ¿Hay regulada la posibilidad de utilizar judicialmente otras herramientas de geolocalización? En caso afirmativo, explique brevemente los requisitos exigibles.

No informa

¿Cómo valora la normativa interna de su país relativa a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos (celulares, tablets, computadoras...)?

No informa

¿Qué obstáculos se encuentran cuando la autoridad judicial de su país ha de acceder a los datos de un proveedor de servicios que está situado en otro Estado?

No informa

¿Qué valor se otorga en su país a la prueba digital (e-evidence) obtenida por Comisión Rogatoria Internacional?

No informa

En su país, ¿es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional?

No informa

¿Considera adecuada la legislación de su país sobre obligación de conservación de datos por las operadoras de comunicación para la investigación y prueba de los delitos?

Si, es adecuada.

¿Tipifica su país bajo un título, capítulo, los ciberdelitos?

No informa.

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

No se encuentran plenamente discriminados en la legislación penal.

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

No se encuentran plenamente discriminados en la legislación penal.

¿Tiene su legislación procesal penal medidas restrictivas de internet (bloqueo, retiro de páginas web, etc.) en materia de ciberdelincuencia económica e intrusiva?

En nuestra normativa penal no existe ninguna medida restrictiva.

¿Pueden los particulares y detectives o investigadores privados utilizar medidas tecnológicas de investigación sin autorización judicial y en qué supuestos?

No pueden sin autorización judicial.

¿Quiénes pueden solicitar y decretar estas medidas?

Las intervenciones telefónicas las solicita el fiscal y las decreta el Juez de Control de Garantías

¿Cuáles son las medidas concretas de investigación con medios tecnológicos que contempla la legislación penal de su país?

El Código Procesal Penal no establece medidas de investigación tecnológica, en la investigación de este tipo de delitos. En su lugar nos fundamentamos en los disposiciones que contienen las actuaciones de ejecución inmediata para la constatación del delito entre las que serían de utilidad el Registro de vehículos, Registro de sitios públicos, Allanamiento de morada, Registros e inspecciones, Depósito y comiso de cosas y documentos, Secuestro de objetos, Incautación, decomiso y destrucción de mercadería falsificada o pirateada, Interceptación de correspondencia.

Se regula la interceptación de las comunicaciones a través de la Ley Especial sobre la Intervención de las Comunicaciones Privadas, que tiene por objeto intervenir escuchas telefónicas a casos concretos determinados por un juez.

En conclusión, se dispone de: 1. Intervención de las comunicaciones, 2. El acceso a sistemas informáticas, mediante previa juramentación de perito si la causa está judicializada previa orden judicial y cuando son peritos ya oficiales y está aún en etapa investigativa no se juramentada. 3. El acceso a la información contenida en dispositivos o bases de datos, al igual se da los vaciados telefónicos con autorización ya sea de la víctima e imputado, 4. La entrega de datos y archivos mediante previa solicitud realizada con control jurisdiccional. 5. Decomiso de ordenadores, computador, CPU etc.

¿Existe en su país una normativa que regula específicamente las medidas de investigación tecnológica restrictivas de derechos fundamentales y cómo la valora?

En Honduras mediante Decreto No. 243-2011 de fecha 8 de diciembre de 2011 se promulgó la Ley especial Sobre intervención de Comunicaciones Privadas, que si bien el artículo 1 establece su finalidad es establecer el marco legal de regulación procedimental de la intervención de las comunicaciones como mecanismo excepcional de investigación a fin de que constituya una herramienta esencial en la lucha contra la criminalidad tradicional y sobre todo contra la criminalidad organizada o no convencional, garantizando el derecho humano de las personas a la comunicación, sin más limitaciones que las dispuestas por la Constitución y las leyes; y que en el capítulo II de las Definiciones y Principios artículo 3 se define como Intervención de las Comunicaciones como una técnica especial de investigación, que consiste en el procedimiento a través del cual, se escucha, capta, registra, guarda, graba, u observa, por parte de la autoridad, sin el consentimiento de sus titulares o participantes, una comunicación que se efectúa, mediante cualquier tipo de transmisión, emisión o recepción de signos, símbolos, señales escritas, imágenes, sonidos, correos electrónicos o información de cualquier naturaleza por hilo, radio-electricidad, medios ópticos u otros medios, sistemas electromagnéticos, telefonía, radio-comunicación, telegrafía, medios informáticos o telemáticos, o de naturaleza similar o análogo, así como la comunicación que se efectúe a través de cualquier medio o tipo de transmisión; en el artículo 2 delimita su objeto a intervenir escuchas telefónicas a casos concretos determinados por un juez, por lo que solo se contienen en la ley los procedimientos para la solicitud, autorización de esta técnica especial de investigación.

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

Al igual que en España se regulan los mismos principios ya mencionados al igual que la Ley de intervención de las comunicaciones aquí en Honduras, son especialidad, legalidad, proporcionalidad, subsidiariedad, control jurisdicción.

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización judicial? ¿Cuál? y ¿Por qué no la exige?

No informa.

¿Es necesario autorización judicial para colocar una baliza en su país? ¿Hay regulada la posibilidad de utilizar judicialmente otras herramientas de geolocalización? En caso afirmativo, explique brevemente los requisitos exigibles.

No informa.

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

En nuestra legislación no se regula o contempla la habilitación legal para la imposición de un micrófono según tengo conocimiento, la intervención de escuchas del investigado si y su ubicación.

¿Cómo valora la normativa interna de su país relativa a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos (celulares, tablets, computadoras...)?

Hay bastante dificultad para obtener este tipo de información y obtención de prueba, siempre se requiere de expertos en la materia, deberían de existir más figuras más leyes que regulen estas acciones, considero que debería existir en nuestra legislación, lo que es el requerimiento inmediato de preservación de los datos que se encuentren en poder de terceros, que pudiera haber una media que ordenó el retiro de material circulando en Internet etc..

¿Qué obstáculos se encuentran cuando la autoridad judicial de su país ha de acceder a los datos de un proveedor de servicios que está situado en otro Estado?

Los problemas que siempre casi se presentan, es que se desconoce a veces los convenios y tratados y el procedimiento para realizar lo que es la asistencia judicial y solicitar la información requerida o prueba a obtener.

¿Qué valor se otorga en su país a la prueba digital (e-evidence) obtenida por Comisión Rogatoria Internacional?

Se le da todo el valor probatorio, sólo se pide que venga apostillado o certificado la información o los medios de prueba requeridos.

En su país, ¿es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional?

Se realiza a través de asistencia judicial, en los casos que tenido conocimiento.

¿Considera adecuada la legislación de su país sobre obligación de conservación de datos por las operadoras de comunicación para la investigación y prueba de los delitos?

Entre las obligaciones de las personas naturales y jurídicas que brindan servicios de comunicación se encuentra la determinada en el artículo 39 Obligación de guardar información por cinco años, que dispone que las compañías que brindan servicios de telefonía, están en la obligación de guardar los datos de todas las conexiones de cada usuario por el plazo de 5 años, la cual en algunas circunstancias no será adecuado ante el término de prescripción de delitos graves.

¿Tipifica su país bajo un título, capítulo, los ciberdelitos?

En México, a partir de 1999, la legislación penal federal tipifica ya algunas conductas como delitos informáticos, sin embargo, no incluye una definición propia de lo que es un delito informático.

Algunos delitos informáticos se encuentran previstos en las leyes que se mencionan a continuación: Ley de Instituciones de Crédito; Ley de Instituciones de Seguros y de Fianzas; Ley del Mercado de Valores; Ley General de Títulos y Operaciones de Crédito; Ley Federal de Protección de Datos Personales en Posesión de los Particulares

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

Partiendo de lo descrito en el Código Penal Federal se tienen los siguientes delitos:

Artículo 424 bis.- Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

> II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación

Artículo 426.- Se impondrá prisión de seis meses a cuatro años y de trescientos a tres mil días multa, en los casos siguientes:

> I. A quien fabrique, modifique, importe, distribuya, venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dic
>
> II. A quien fabrique o distribuya equipo destinado a la recepción de una señal de cable encriptada portadora de programas, sin autorización del distribuidor legítimo de dicha señal.

Artículo 427 Ter.- A quien, con fines de lucro, fabrique, importe, distribuya, rente o de cualquier manera comercialice dispositivos, productos o componentes destinados a eludir una medida tecnológica de protección efectiva que utilicen los productores de fonogramas, artistas, intérpretes o ejecutantes, así como los autores de cualquier obra protegida por el derecho de autor o derecho conexo, se le impondrá de seis meses a seis años de prisión y de quinientos a mil días multa.

Así mismo, de acuerdo con el Código Penal para el estado de Veracruz se tienen los siguientes delitos:

Engaño Telefónico y Suplantación De Identidad. Artículo 173 bis. A quien con el propósito de obtener un lucro para sí o para otro, a través de una llamada telefónica o por cualquier medio electrónico, pretenda engañar a una persona haciéndole creer que le va a causar o le está causando un daño a un tercero, se le aplicarán de tres a diez años de prisión y multa de quinientos a mil días de salario.

Igual penalidad se aplicará si quien realiza la llamada o envía el mensaje electrónico pretende hacer creer al receptor que le causará un daño o que se ha privado de la libertad a una persona. Este delito se perseguirá de oficio.

Artículo 283 Ter. Serán equiparables al delito de suplantación de identidad y se impondrán las mismas penas previstas en el artículo que precede, las siguientes conductas:

> III. A quien, a través de Internet o cualquier otro medio de comunicación, suplante la identidad de una persona física o jurídica que no le pertenezca;

V. Al que use claves bancarias o de banca electrónica, sin la autorización de su titular u obtenidas de forma ilegal, para obtener un beneficio propio o para algún tercero

Seguidamente, atendiendo la Ley de Instituciones de Crédito, se conocen las siguientes tipificaciones:

Artículo 112 Bis.- Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello, respecto de tarjetas de crédito, de débito, cheques, formatos o esqueletos de cheques o en general cualquier otro instrumento de pago, de los utilizados o emitidos por instituciones de crédito del país o del extranjero:

IV.- Altere, copie o reproduzca la banda magnética o el medio de identificación electrónica, óptica o de cualquier otra tecnología, de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

VI. Posea, adquiera, utilice o comercialice equipos o medios electrónicos, ópticos o de cualquier otra tecnología para sustraer, copiar o reproducir información contenida en alguno de los objetos a que se refiere el párrafo primero de este artículo, con el propósito de obtener recursos económicos, información confidencial o reservada.

Artículo 112 Quáter.- Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello:

> I. Acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada,
>
> II. Altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada

Artículo 112 Sextus.- Se sancionará con prisión de tres a nueve años y multa de treinta mil a trescientas mil Unidades de Medida y Actualización, a quien valiéndose de cual-

quier medio físico, documental, electrónico, óptico, magnético, sonoro, audiovisual o de cualquier otra clase de tecnología, suplante la identidad, representación o personalidad de una autoridad financiera o de alguna de sus áreas o de alguno de los sujetos a que se refiere el artículo 3 de esta Ley, o de un servidor público, directivo, consejero, empleado, funcionario, o dependiente de éstas, en los términos establecidos por el artículo 116 Bis 1 de la presente Ley.

En atención a lo regulado en la ley Federal de Protección de Datos Personales en Posesión de los Particulares, tipifica como delitos las siguientes conductas:

Capítulo XI de los Delitos en Materia del Tratamiento Indebido de Datos Personales
Artículo 67.- Se impondrán de tres meses a tres años de prisión al que, estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

En materia de ciberdelincuencia intrusiva la legislación penal mexicana contempla las siguientes figuras:

Sobre los delitos relacionados con Revelación de secretos y acceso ilícito a sistemas y equipos de informática en su capítulo II para delitos de Acceso ilícito a sistemas y equipos de informática contempla:

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público

en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa. A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero

¿Cuáles son las medidas concretas de investigación con medios tecnológicos que contempla la legislación penal de su país?

En materia investigativa la legislación procesal penal mexicana contempla lo siguiente:

Artículo 252. Actos de investigación que requieren autorización previa del Juez de control Con excepción de los actos de investigación previstos en el artículo anterior, requieren de autorización previa del Juez de control todos los actos de investigación que impliquen afectación a derechos establecidos en la Constitución, así como los siguientes:

III. La intervención de comunicaciones privadas y correspondencia;

Artículo 291. Intervención de las comunicaciones privadas
Cuando en la investigación el Ministerio Público considere necesaria la intervención de comunicaciones privadas, el Titular de la Procuraduría General de la República, o en quienes éste delegue esta facultad, así como los Procuradores de las entidades federativas, podrán solicitar al Juez federal de control competente, por cualquier medio, la autorización para practicar la intervención, expresando el objeto y necesidad de la misma. Párrafo reformado DOF 17-06-2016

La intervención de comunicaciones privadas abarca todo sistema de comunicación, o programas que sean resultado de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real.
La solicitud deberá ser resuelta por la autoridad judicial de manera inmediata, por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público, en un plazo que no exceda de las seis horas siguientes a que la haya recibido.

También se requerirá autorización judicial en los casos de extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos.

Artículo 292. Requisitos de la solicitud. La solicitud de intervención deberá estar fundada y motivada, precisar la persona o personas que serán sujetas a la medida; la identificación del lugar o lugares donde se realizará, si fuere posible; el tipo de comunicación a ser intervenida; su duración; el proceso que se llevará a cabo y las líneas, números o aparatos que serán intervenidos, y en su caso, la denominación de la empresa concesionada del servicio de telecomunicaciones a través del cual se realiza

la comunicación objeto de la intervención. El plazo de la intervención, incluyendo sus prórrogas, no podrá exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse nuevas intervenciones cuando el Ministerio Público acredite nuevos elementos que así lo justifiquen.

Artículo 294. Objeto de la intervención. Podrán ser objeto de intervención las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como por cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores. En ningún caso se podrán autorizar intervenciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su Defensor. El Juez podrá en cualquier momento verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total.

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

No informa

¿Quiénes pueden solicitar y decretar estas medidas?

No informa

¿Tiene su legislación procesal penal medidas restrictivas de internet (bloqueo, retiro de páginas web, etc.) en materia de ciberdelincuencia económica e intrusiva?

No informa

¿Pueden los particulares y detectives o investigadores privados utilizar medidas tecnológicas de investigación sin autorización judicial y en qué supuestos?

No informa

¿Existe en su país una normativa que regula específicamente las medidas de investigación tecnológica restrictivas de derechos fundamentales y cómo la valora?

No existe alguna regulación sobre investigación en tecnológica en México, solo se señala la en el Código Nacional de Procedimientos Penales, la intervención de comunicaciones, la cual se realiza con control judicial.

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización judicial? ¿Cuál? y ¿Por qué no la exige?

No informa

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

No informa.

¿Es necesario autorización judicial para colocar una baliza en su país? ¿Hay regulada la posibilidad de utilizar judicialmente otras herramientas de geolocalización? En caso afirmativo, explique brevemente los requisitos exigibles.

No informa.

¿Qué obstáculos se encuentran cuando la autoridad judicial de su país ha de acceder a los datos de un proveedor de servicios que está situado en otro Estado?

El tiempo que se lleva realizar una investigación con Asistencia Jurídica Internacional, que en promedio tarda entre 6 y 8 meses y eso retrasa las investigaciones o compromete el éxito de estas.

¿Qué valor se otorga en su país a la prueba digital (e-evidence) obtenida por Comisión Rogatoria Internacional?

Tiene valoración plena cuando ha llevado las formalidades de la Asistencia Jurídica Internacional, toda vez que si se obtiene de manera "económica" o informal con alguna agencia de inteligencia o de investigación gubernamental de otro país, no tendrá valor probatorio.

¿Cómo valora la normativa interna de su país relativa a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos (celulares, tablets, computadoras...)?

Buena, dado a que la Ley de Telecomunicaciones contempla lo siguiente:
Artículo 44. Los concesionarios de redes públicas de telecomunicaciones deberán:
XII. Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos:

a) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);

b) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;

c) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;

d) Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la eti-

queta de localización (identificador de celda) desde la que se haya activado el servicio; e) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y

f) La obligación de conservación de datos a que se refiere la presente fracción cesa a los doce meses, contados a partir de la fecha en que se haya producido la comunicación.

Los concesionarios tomarán las medidas técnicas necesarias respecto de los datos objeto de conservación, que garanticen su conservación, cuidado, protección, no manipulación o acceso ilícito, destrucción, alteración o cancelación, así como el personal autorizado para su manejo y control.

En su país, ¿es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional?

No, el juez de control autoriza el acto de investigación y el Fiscal Federal es quien los solicita.

¿Considera adecuada la legislación de su país sobre obligación de conservación de datos por las operadoras de comunicación para la investigación y prueba de los delitos?

Si, por que la ley de federal de telecomunicaciones contempla las obligaciones para los proveedores de red.

NICARAGUA

¿Tipifica su país bajo un título, capítulo, los ciberdelitos?

No informa

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

No informa

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

No informa

¿Tiene su legislación procesal penal medidas restrictivas de internet (bloqueo, retiro de páginas web, etc.) en materia de ciberdelincuencia económica e intrusiva?

No informa

¿Quiénes pueden solicitar y decretar estas medidas?

La citada Ley en el Art. 39 hace referencia a la autorización judicial y establece que en la etapa de investigación para la obtención y conservación de la información contenida en los sistemas informáticos o cualquiera de sus componentes, se requerirá autorización judicial por cualquier Juez de Distrito de lo Penal, a petición debidamente fundamentada por la Policía Nacional o el Ministerio Público. Una vez iniciado el proceso, cualquiera de las partes podrá solicitar la autorización al Juez de la causa.

¿Pueden los particulares y detectives o investigadores privados utilizar medidas tecnológicas de investigación sin autorización judicial y en qué supuestos?

No informa

¿Cuáles son las medidas concretas de investigación con medios tecnológicos que contempla la legislación penal de su país?

La Ley 1042, Ley Especial de Ciberdelitos en Nicaragua, establece en el capítulo VI los procedimientos y las medidas, determinándose entre otras, que se haga la entrega inmediata ya sea a la persona natural y jurídica, de la información que se encuentre en un sistema de información o en cualquiera de sus componentes;

La preservación y mantenimiento de la integridad del sistema de información o de cualquiera de sus componentes, conservar los datos de tráfico, conexión, acceso o cualquier otra información que se encuentre en su poder o bajo su control y que pueda ser de utilidad a la investigación. Tomar en secuestro o asegurar un sistema de información o cualquiera de sus componentes, en todo o en parte.

Realizar y retener copia del contenido del sistema de información o de cualquiera de sus componentes; realizar la intervención o interceptación de las telecomunicaciones en tiempo real, según el procedimiento establecido en el artículo 62 de la Ley Nº. 735, Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados, el cual será aplicable a los delitos contenidos en la presente Ley.

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

No informa

¿Existe en su país una normativa que regula específicamente las medidas de investigación tecnológica restrictivas de derechos fundamentales y cómo la valora?

La Constitución Política de Nicaragua, establece como derecho de todo ciudadano a tener una vida privada, y es el Estado el que tutela y garantiza ese derecho fundamental, Art. 26 y 34.11 Cn.

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización judicial? ¿Cuál? y ¿Por qué no la exige?

No informa

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

No informa

En su país, ¿es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional?

No informa

¿Qué obstáculos se encuentran cuando la autoridad judicial de su país ha de acceder a los datos de un proveedor de servicios que está situado en otro Estado?

No informa

¿Es necesario autorización judicial para colocar una baliza en su país? ¿Hay regulada la posibilidad de utilizar judicialmente otras herramientas de geolocalización? En caso afirmativo, explique brevemente los requisitos exigibles.

No informa

¿Cómo valora la normativa interna de su país relativa a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos (celulares, tablets, computadoras...)?

No informa

¿Considera adecuada la legislación de su país sobre obligación de conservación de datos por las operadoras de comunicación para la investigación y prueba de los delitos?

Es adecuada, por cuánto va dirigida única y exclusivamente para demostrar hechos o conductas ilícitas sometidas a un proceso, por lo que, dicha conservación no será permanente, sino hasta cuando dicho proceso termine. La Ley Especial de Ciberdelito, Ley 1042 establece en el art. 39 que el Juez tiene la potestad de ordenar a una persona natural o jurídica preservar y mantener la integridad de un sistema de información o de cualquiera de sus componentes, conservar los datos de tráfico, conexión, acceso o cualquier otra información que se encuentre en su poder o bajo su control y que pueda ser de utilidad a la investigación, por un período de hasta noventa (90) días, pudiendo esta orden ser renovada una sola vez por el mismo plazo.

¿Tipifica su país bajo un título, capítulo, los ciberdelitos?

No informa

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

De acuerdo a nuestro código penal vigente, el cual fue aprobado mediante ley 14 del 18 de mayo de 2007, en su Título VIII, regula los delitos contra la Seguridad Jurídica de los Medios Electrónicos, es decir los delitos contra la seguridad informática. Del artículo 289 al 292 regula las siguientes conductas delictivas y sus respectivas penas: a) ingresar o utilizar de bases de datos, red o sistemas informáticos y, b) apoderar, copiar, utilizar o modificar datos en tránsito o contenidos en bases de datos o sistemas informáticos, o interferir, interceptar, obstaculizar o impedir la transmisión. Además, determina ciertas conductas como circunstancias agravantes que aumentan la pena de prisión.

Este título fue ubicado por el legislador en el Código Penal, entre los títulos que tipifican los Delitos contra el Orden Económico y los Delitos Contra la Seguridad Colectiva, lo cual refleja sus consideraciones en torno a la extensión de daños que pueden llegar a generar esta variedad de conductas delictivas.

Iniciamos con el tipo objetivo contenido en el artículo 289, respecto al cual en primer lugar
tenemos que la acción típica consiste tanto en ingresar como utilizar las bases de datos, redes o sistemas informáticos. Estos verbos rectores difieren de tal manera que entendemos que el legislador buscó la protección tanto de los medios de seguridad informática como de la información que estos resguardan.

En este orden de ideas, en lo relativo al objeto material, tenemos las bases de datos, redes
y sistemas informáticos y la información. Los bienes jurídicos protegidos son: la intimidad, la honra, la fe pública, la económica, la propiedad intelectual, las comunicaciones, los medios de transporte y la seguridad pública, entre otros.

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

En la legislación panameña el artículo 289 es la referencia mas expresiva de esta forma de ciberdelincuencia. Este consiste tanto en ingresar como utilizar las bases de datos, redes o sistemas informáticos. Estos verbos rectores difieren de tal manera que entendemos que el legislador buscó la protección tanto de los medios de seguridad informática como de la información que estos resguardan.

¿Tiene su legislación procesal penal medidas restrictivas de internet (bloqueo, retiro de páginas web, etc.) en materia de ciberdelincuencia económica e intrusiva?

En este punto como medida restrictiva de Internet, en si no hay, pero podemos observar el artículo 50 del Código Penal, referente a las penas sustitutivas como la inhabilitación para el ejercicio de determinada profesión, oficio, industria o comercio, lo cual podría adecuarse a que el juez pueda bloquear el acceso a cualquier medio electrónico de ser conductas retiradas de estos delitos, si bien el mismo se comete utilizando este medio.

De igual forma en el artículo 270 del Código Procesal Penal, se establecen las Medidas conservatorias innominadas. Cuando existan motivos justificados para temer que, mientras dure el proceso, puedan continuar las situaciones que facilitan la comisión del delito, a solicitud de parte y con prueba suficiente, el Juez podrá ordenar las medidas conservatorias, de protección o de suspensión apropiadas, según las circunstancias, para prevenir los efectos del delito.

Así mismo en el artículo 336 del Código Procesal Penal se establece otras medidas de protección, para salvaguardar la integridad de las víctimas, los testigos, los peritos y otros intervinientes en el proceso penal, donde podrán aplicarse la entrega de celulares o teléfonos móviles.

¿Cuáles son las medidas concretas de investigación con medios tecnológicos que contempla la legislación penal de su país?

Dentro de las herramientas investigativas con las que dispone el estado panameño se destacan por su aplicabilidad al contexto de la cibercriminalidad los siguientes:

1) Aprehensión Provisional de medios informáticos procedentes o relacionados al delito Aprehensión Provisional de Bienes. Este se encuentra desarrollado en los siguientes términos:

Artículo 252. Aprehensión provisional. Serán aprehendidos provisionalmente por el funcionario de instrucción los instrumentos, los bienes muebles e inmuebles, los valores y los productos derivados o relacionados con la comisión de delitos contra la Administración Pública, de blanqueo de capitales, financieros, contra la propiedad intelectual, seguridad informática, extorsión, secuestro, pandillerismo, sicariato, terrorismo y financiamiento del terrorismo, de narcotráfico y delitos conexos, contra la trata de personas y delitos conexos, contra la trata de personas y delitos conexos, delincuencia organizada, tráfico ilícito de migrantes y delitos conexos y quedarán a órdenes de Ministerio de Economía y Finanzas hasta que la causa sea decidida por el Juez competente.

2) Intercepción de comunicaciones. Mismo que se encuentra descrito en los siguientes términos:

Artículo 311. Interceptación de comunicaciones. La interceptación o grabación por cualquier medio técnico de otras formas de comunicación personal requieren de autorización judicial.

A solicitud del Fiscal, el Juez de Garantías podrá, atendiendo a la naturaleza del caso, decidir si autoriza o no la grabación de las conversaciones e interceptación de comunicaciones cibernéticas, seguimientos satelitales, vigilancia electrónica y comunicaciones telefónicas para acreditar el hecho punible y la vinculación de determinada persona.

La intervención de las comunicaciones tendrá carácter excepcional. En caso de que se autorice lo pedido, el juzgador deberá señalar un término que no exceda de los veinte días y solo podrá ser prorrogado a petición del Ministerio Público, que deberá explicar los motivos que justifican la solicitud.

A quien se le encomiende interceptar y grabar la comunicación o quien la escriba tendrá la obligación de guardar secreto sobre su contenido, salvo que, citado como testigo en el mismo procedimiento, se le requiera responder sobre ella.

El material recabado en la diligencia y conservado en soporte digital deberá permanecer guardado bajo una cadena de custodia.

Las transcripciones de las grabaciones e informaciones receptadas constarán en un acta en la que solo se debe incorporar lo que guarde relación con el caso investigado, la que será firmada por el Fiscal.

3) Incautación de Datos Informáticos. Descrito en los siguientes términos:

Artículo 314. Incautación de datos. Cuando se incauten equipos informáticos o datos almacenados en cualquier otro soporte, regirán las mismas limitaciones referidas al secreto profesional y a la reserva sobre el contenido de los documentos incautados.
El examen del contenido de los datos se cumplirá bajo la responsabilidad del Fiscal que lo realiza. A dicha diligencia se citará, con la debida antelación, a la persona imputada y su defensor. Sin embargo, la ausencia de ellos no impide la realización del acto.
El equipo o la información que no resulten útiles a la investigación o comprendidos como objetos no incautables serán devueltos de inmediato y no podrán utilizarse para la investigación

Estas medidas solo las puede solicitar el Fiscal del Ministerio Público de Panamá ante el Juez de Garantías competente, quien tutela los derechos fundamentales, tanto de la víctima, como del imputado durante la fase de investigación de 6 meses.

Ningún particular puede solicitar estas medidas de restricción en el proceso penal panameño. Hacer lo contrario, sin intervención del Fiscal ni autorización del Juez constituiría un delito Contra la Libertad en nuestro ámbito jurídico.

En Panamá al tenor de lo preceptuado en el artículo 12 del Código Procesal Penal, que preceptúa el Control judicial de afectación de derechos fundamentales, se indica claramente que las medidas de coerción, restrictivas de la libertad personal o de otros derechos son excepcionales. y que el Juez de Garantías, al decretar alguna de estas medidas, observará el carácter excepcional, subsidiario, provisional, proporcional y humanitario de éstas.

La tercera de las medidas detalladas ut supra no requiere de autorización judicial previa, toda vez que tal cual lo establece nuestra legislación adjetiva punitiva, la incautación de datos informáticos, es un acto de investigación con control posterior del Juez de Garantías y a diferencia de las otras dos, permite la participación de la defensa en la materialización de la diligencia, a efectos de asegurar el derecho a la intimidad y demás garantías fundamentales

¿Quiénes pueden solicitar y decretar estas medidas?

Estas medidas que requieren control previo, las solicita el Fiscal ante el Juez de Garantías en turno, quien las resolverá en el menor termino posible

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

No en la actualidad dentro del procedimiento penal panameño no se dispone de esa técnicas de investigación.

¿Pueden los particulares y detectives o investigadores privados utilizar medidas tecnológicas de investigación sin autorización judicial y en qué supuestos?

No solo el Fiscal o los agentes del Ministerio Público facultados, los particulares e investigadores privados, no están autorizados, y los detectives se rigen bajo la dirección del Ministerio Público.

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

El mismo se debe regir bajos del debido proceso, contradicción, inmediación, simplificación, eficacia, oralidad, publicidad, concentración, estricta igualdad de las partes, economía procesal, legalidad, constitucionalización del proceso y derecho de defensa.

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización

Si, como medida tecnológica de investigación se pueda usar la incautación de datos. Es decir que se pueden incautar equipos informáticos o datos almacenados en cualquier otro soporte, siempre y cuando se haga conforme a las mismas limitaciones del secreto profesional y a la reserva sobre el contenido de los documentos incautados.

Este examen del contenido de los datos se hace bajo la responsabilidad del Fiscal. Solo que debe someterlo a control posterior ante el Juez de Garantías, en un término de 10 días.

La medida de incautación de datos, ya que es una acto de investigación propio del Fiscal, y está dentro de los actos de Investigación con control posterior ante el Juez de Garantías.

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

El mismo se debe regir bajos del debido proceso, contradicción, inmediación, simplificación, eficacia, oralidad, publicidad, concentración, estricta igualdad de las partes, economía procesal, legalidad, constitucionalización del proceso y derecho de defensa.

¿Existe en su país una normativa que regula específicamente las medidas de investigación tecnológica restrictivas de derechos fundamentales y cómo la valora?

El Código Procesal Penal de Panamá establece las normas que regula las medidas de investigación tecnológica en el artículo 310 que establece que, para la incautación de correspondencia epistolar, telegráfica y otros documentos privados, se requiere autorización judicial previa. La otra norma que contempla el Código Penal es el artículo 311 se refiere a la interceptación de comunicaciones, los cuales son actos de investigación que requieren autorización previa del Juez de Garantías, la cual debe hacerse por escrito antes el Juez.

La otra norma vigente en nuestro Código Procesal Penal es la establecida en el artículo 314 referente a la Incautación de datos la cual debe someterse a control posterior ante el Juez de Garantía s en un término de 10 días hábiles una vez se reciba la información y es en audiencia ante el Juez de Garantías que se legaliza la información, en casos cuando haya que legalizar la información obtenida de las telefónicas que operan en nuestro país como es el caso de las empresas Claro, Digicel, Mas Móvil y Tigo (Anteriormente Movistar).

Lo anterior con fundamento en la Ley 51 del 18 de septiembre del 2009, la cual dicta normas para la conservación de datos de los usuarios de los servicios de telecomunicaciones y adopta otras disposiciones. Es importante señalar esto en vista que el único facultado para autorizar una diligencia de inspección ocular y extracción de datos en equipos celulares, tablets, computadoras, dispositivos USB y otros equipos electrónicos es el Juez de Garantías.

De obtenerse información relevante para la investigación se solicita a los analistas de la Dirección de Investigación Judicial, que es un organismo policial que funciona como brazo auxiliar en las investigaciones se realice el análisis de cruce de llamadas.

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización judicial? ¿Cuál? y ¿Por qué no la exige?

Si, como medida tecnológica de investigación se pueda usar la incautación de datos. Es decir que se pueden incautar equipos informáticos o datos almacenados en cualquier otro soporte, siempre y cuando se haga conforme a las mismas limitaciones del secreto profesional y a la reserva sobre el contenido de los documentos incautados.

Este examen del contenido de los datos se hace bajo la responsabilidad del Fiscal. Solo que debe someterlo a control posterior ante el Juez de Garantías, en un término de 10 días.

La medida de incautación de datos, ya que es una acto de investigación propio del Fiscal, y está dentro de los actos de Investigación con control posterior ante el Juez de Garantías.

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

No en la actualidad dentro del procedimiento penal panameño no se dispone de esa técnicas de investigación.

¿Es necesario autorización judicial para colocar una baliza en su país? ¿Hay regulada la posibilidad de utilizar judicialmente otras herramientas de geolocalización? En caso afirmativo, explique brevemente los requisitos exigibles.

De igual forma que en lo anterior, Panamá no cuenta con esa esas técnicas de investigación, las autoridades solo pueden apoyarse en las empresas telefónicas, para que ellas brinden la información de ubicación de acuerdo a la señal telefónica emita por los dispositivos móviles, esa es la única forma de geolocalización.

¿Cómo valora la normativa interna de su país relativa a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos (celulares, tablets, computadoras...)?

Desde el año 2008, a partir de la incorporación de los Servicios de Criminalística al Instituto de Medicina Legal y Ciencias Forenses, se produjo una reorganización administrativa, y se previó la necesidad de elaborar un Manual de Procedimientos del Sistema de Cadena de Custodia e implementarlo, con base en las nuevas técnicas de investigación científica, los tratados internacionales sobre Derechos Humanos, la Constitución Política y las normas respectivas. Entendiendo el papel primordial que tiene la cadena de custodia en el nuevo Sistema Penal Acusatorio, que ha entrado en vigencia en nuestro país, esto en atención al artículo 28 de la Ley 69 de 27 de diciembre de 2007, donde establece que

es función del instituto iniciar y mantener, en coordinación con la Dirección de Investigación Judicial, la cadena de custodia de todos los instrumentos, objetos y demás elementos relacionados con el hecho punible, así como lo necesario para identificar a los autores, cómplices del delito.

¿Qué obstáculos se encuentran cuando la autoridad judicial de su país ha de acceder a los datos de un proveedor de servicios que está situado en otro Estado?

En el contexto panameño siempre se presentan dificultades por los diferentes trámites que se requieren, pero la experiencia no es del todo negativa ya que por el acceso y punto geográfico que disfruta, muchas veces contribuye a que se facilitan los procesos de obtención de la información.

¿Qué valor se otorga en su país a la prueba digital (e-evidence) obtenida por Comisión Rogatoria Internacional?

En años recientes Panamá ha vivido una cargada experiencia con los famosos casos de Odebrecht, en donde se utilizaron comisiones rogatorias internacionales, a las cuales se le otorgó toda su validez, para probar las conductas punibles investigadas.

En su país, ¿es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional?

No es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional, ya que el Juez de Garantías o el Tribunal de Juicio no podrán decretar, en ningún caso, pruebas de oficio. Esa función recae exclusivamente en el Fiscal.

¿Considera adecuada la legislación de su país sobre obligación de conservación de datos por las operadoras de comunicación para la investigación y prueba de los delitos?

En Panamá las empresas telefónicas que prestan este tipo de servicio como Mas Móvil, Claro, Digicel y Tigo (anteriormente Movistar), que es donde se solicitan con mayor frecuencia los datos de las teléfonos móviles de las personas investigadas y de las víctimas, tienen un tiempo para mantener en sus bases de datos y poderlas proporcionar a las autoridades de máximo de 6 meses. Esta información es solicitada previa resolución motivada de manera oficiosa o se realiza en la misma empresa o levantando el acta correspondiente, para luego legalizar ante el Juez de Garantías la información obtenida en un plazo legal de 10 días hábiles a partir del momento de recibida la información o se practique la diligencia de inspección en las empresas telefónicas

¿Tipifica su país bajo un título, capítulo, los ciberdelitos?

No informa.

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

No informa.

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación? ¿Tiene su legislación procesal penal medidas restrictivas de internet (bloqueo, retiro de páginas web, etc.) en materia de ciberdelincuencia económica e intrusiva?

No informa.

¿Pueden los particulares y detectives o investigadores privados utilizar medidas tecnológicas de investigación sin autorización judicial y en qué supuestos?

No informa.

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

No informa.

¿Cuáles son las medidas concretas de investigación con medios tecnológicos que contempla la legislación penal de su país?

El Código Procesal Penal del Paraguay dispone de herramientas para la obtención de información que conlleve a llegar a la verdad real sobre los ciberdelitos; lo anterior siempre bajo el pedido del órgano investigador que es el Ministerio Publico y bajo el control jurisdiccional del Juez Penal de Garantías, atendiendo los siguientes artículos:

Art. 192 . Operaciones Técnicas. Para mayor eficacia y calidad de los registros e inspecciones, se podrá ordenar operaciones técnicas o científicas, reconocimientos y reconstrucciones. Si el imputado decide participar en la diligencia regirá las reglas previstas para su declaración (estar en compañía de su Abogado Defensor y exonerado de decir verdad). Para la participación de testigos, peritos e intérpretes, regirá las disposiciones establecidas por este Código.

De igual forma Art. 200. Señala sobre la Intervención de Comunicaciones, que el juez podrá ordenar por resolución fundada, bajo pena de nulidad, la intervención de las comunicaciones del imputado, cualquiera sea el medio técnico utilizado para conocerla. El resultado solo podrá ser entregado al Juez que la ordeno, quien procederá examinando el contenido y si guarda relación con el hecho investigado ordenara el secuestro caso contrario dispondrá la entrega al destinario, labrando un acto de todo lo actuado, tal como lo dispone el art. 199 C.P.P. cuando expresa que podrá ordenar la versión escrita de la grabación o de

aquellas partes que considere útil y ordenara la destrucción de toda la grabación o de las partes que no tengan relación con el procedimiento, previo acceso a ellas del Ministerio Publico, del imputado y su defensor. La intervención de la comunicación será excepcional.

¿Quiénes pueden solicitar y decretar estas medidas?

Se encuentran legitimados para elevar solicitud el Ministerio Público y la decreta el Juez de Control de Garantías.

¿Existe en su país una normativa que regula específicamente las medidas de investigación tecnológica restrictivas de derechos fundamentales y cómo la valora?

En Paraguay la aplicación de algún tipo de medida restrictiva de los derechos fundamentales sólo puede realizarse mediante orden judicial, conforme lo dispuesto en el artículo 282 del C.P.P, que establece el control judicial a las actuaciones del Ministerio Público y de la Policía de acuerdo a las garantías establecidas en la Constitución, en el Derecho Internacional vigente y en el C.P.P.

No poseen normativa específica pues no todas las medidas se encuentran previstas; aunque a la presente fecha se encuentra bajo estudio por parte de la Comisión de Reforma Penal. En conclusión, se dispone de lo siguiente: Los artículos 172 (búsqueda de la verdad); 173 (libertad probatoria) y 175 (exclusiones probatorias) son las utilizadas para fundamentar los pedidos de exclusión de aquellos actos que no reúnan los requisitos exigidos.

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización judicial? ¿Cuál? y ¿Por qué no la exige?

No informa.

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

No informa.

¿Es necesario autorización judicial para colocar una baliza en su país? ¿Hay regulada la posibilidad de utilizar judicialmente otras herramientas de geolocalización? En caso afirmativo, explique brevemente los requisitos exigibles.

No informa.

¿Cómo valora la normativa interna de su país relativa a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos (celulares, tablets, computadoras...)?

No informa.

¿Qué obstáculos se encuentran cuando la autoridad judicial de su país ha de acceder a los datos de un proveedor de servicios que está situado en otro Estado?

No informa.

¿Qué valor se otorga en su país a la prueba digital (e-evidence) obtenida por Comisión Rogatoria Internacional?

No informa.

En su país, ¿es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional?

No informa.

¿Considera adecuada la legislación de su país sobre obligación de conservación de datos por las operadoras de comunicación para la investigación y prueba de los delitos?

En cuanto a la conservación de datos, por resolución n°1350/2002 de la Comisión Nacional de Telecomunicaciones (CONATEL), se estableció el plazo de seis meses como período obligatorio de conservación de los registros de detalles de llamadas.

Consideramos que dicho plazo debería extenderse pues existen investigaciones complejas como lo de crimen organizado, narcotráfico y transnacionales que requieren mayor tiempo de conservación.

¿Tipifica su país bajo un título, capítulo, los ciberdelitos?

En Perú está regulado en la Ley N°30096, Ley de delitos informáticos, del 21 de octubre de 2013, modificada por la Ley N°30171, de fecha 17 de febrero de 2014.
Asimismo, entre la legislación relevante en materia de criminalización de la ciberdelincuencia, así como en cuanto a proveer un marco jurídico para su persecución se encuentran:

- Ley N°30077, Ley contra el crimen organizado, del 19 de agosto del 2013.

- Ley N°27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional, de fecha 10 de abril de 2002, modificada por la Ley N°30096 del 2013, que agrega los delitos informáticos a la lista de delitos en que los jueces tendrán la facultad cons-

En cuanto a la conservación de datos, por resolución n°1350/2002 de la Comisión Nacional de Telecomunicaciones (CONATEL), se estableció el plazo de seis meses como período obligatorio de conservación de los registros de detalles de llamadas.

Consideramos que dicho plazo debería extenderse pues existen investigaciones complejas como lo de crimen organizado, narcotráfico y transnacionales que requieren mayor tiempo de conservación.

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

En Perú está regulado en el Título V Delitos contra el patrimonio, capítulo X como Delitos Informáticos, en los Artículos 207-A.- Interferencia, acceso o copia ilícita contenida en base de datos, 207-B.- Alteración, daño o destrucción de base de datos, 207-Circunstancias calificantes agravantes, y, 207-D.- Tráfico Ilegal de datos.

Al respecto es preciso destacar que el Código Penal peruano no desarrolla sistemáticamente los elementos descriptivos de los tipos penales de los delitos informáticos, siendo a la fecha leve el desarrollo del derecho sustantivo en ese sentido. Este ultimo aspecto es motivo de reflexión académica en la medida que resulta relevante trazar como objetivo el cumplimiento de los compromisos y pautas perfiladas por la convención contra la cibercriminalidad del consejo europeo (CETS 185) conocida como Convención de Budapest.

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

No informa.

¿Tiene su legislación procesal penal medidas restrictivas de internet (bloqueo, retiro de páginas web, etc.) en materia de ciberdelincuencia económica e intrusiva?

La Ley Nº 300077, en su Capítulo III, comprende medidas limitativas de derecho, el cual es el Levantamiento del Secreto Bancario, reserva tributaria y bursátil. El valor probatorio de la prueba trasladada está sujeto a la evaluación que el órgano judicial realice de todas las pruebas actuadas durante el proceso en que ha sido incorporada, respetando las reglas de la sana crítica, la lógica, las máximas de la experiencia y los conocimientos científicos.

¿Quiénes pueden solicitar y decretar estas medidas?

Las medidas especiales de investigación tecnológicas son solicitadas por el Ministerio Público – el Fiscal es quien mediante requerimiento debidamente motivado y siempre que exista elementos de convicción suficientes, solicita autorización para ejecutar medidas especiales de investigación y es el juez, excepcionalmente a pedido del Fiscal, quien autoriza las medidas restrictivas de derechos.

¿Cuáles son las medidas concretas de investigación con medios tecnológicos que contempla la legislación penal de su país?

El Código Procesal Penal no establece medidas de investigación tecnológica, en la investigación de este tipo de delitos la autoridad judicial se fundamenta en las disposiciones que contienen las actuaciones de ejecución inmediata para la constatación del delito entre las que serían de utilidad el Registro de vehículos, Registro de sitios públicos, Allanamiento de morada, Registros e inspecciones, Depósito y comiso de cosas y documentos, Secuestro de objetos, Incautación, decomiso y destrucción de mercadería falsificada o pirateada, Interceptación de correspondencia.

Se regula la interceptación de las comunicaciones a través de la Ley Especial sobre la Intervención de las Comunicaciones Privadas, que tiene por objeto intervenir escuchas telefónicas a casos concretos determinados por un juez.

¿Pueden los particulares y detectives o investigadores privados utilizar medidas tecnológicas de investigación sin autorización judicial y en qué supuestos?

No están legitimados. Sin embargo, en Perú existe un Proyecto Ley Nº 7335/2020-CR, el cual cuenta con la Ley General de Detectives Privados del Perú, y está contemplado por la Constitución Política del Perú de 1993, Reglamento del Congreso de la

Republica y el Decreto Supremo 053-84-IN, aprobando el Reglamento de Detectives Privados.

La actividad del detective privado a prestar servicios profesionales de carácter civil, comercial y otras de naturaleza análoga, que no sea competencia de la Policía Nacional del Perú; sin embargo, los detectives privados en el desempeño de sus labores, no pueden utilizar medidas o técnicas tecnológicas de investigación, estrictamente tienen que regirse en su reglamento.

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización judicial? ¿Cuál? y ¿Por qué no la exige?

En la legislación peruana, todas las medidas o técnicas especiales de investigación, tienen que ser requeridas y autorizadas por la autoridad competente. Todas tienen que ser autorizadas.

¿Qué obstáculos se encuentran cuando la autoridad judicial de su país ha de acceder a los datos de un proveedor de servicios que está situado en otro Estado?

La conservación de datos debe formar parte de la estrategia inicial de investigación, con miras a utilizar la cooperación directa o la solicitud de asistencia judicial internacional. Si no se conserva la información, ésta se corre el riesgo de ser eliminada o suprimida.

¿Existe en su país una normativa que regula específicamente las medidas de investigación tecnológica restrictivas de derechos fundamentales y cómo la valora?

El artículo VI del T.P. del Código Procesal Penal peruano, establece la observancia del principio de legalidad en las medidas limitativas de derechos fundamentales, salvo las excepciones previstas en la Constitución, sólo podrán dictarse por la autoridad judicial, en el modo, forma y con las garantías previstas por la Ley, además de que el Juez impondrá mediante resolución motivada, a instancia de la parte procesal legitimada, y que la orden judicial debe sustentarse en suficientes elementos de convicción, en atención a la naturaleza y finalidad de la medida y al derecho fundamental objeto de limitación, así como respetar el principio de proporcionalidad.

Siendo así, el Código Procesal Penal peruano que sigue el modelo acusatorio garantista, establece como medidas tecnológicas de investigación criminal la restricción de derechos como medidas idóneas para lograr los fines de esclarecimiento del hecho y en la medida que sean necesarias, urgentes, racionales y proporcionales y existan suficientes elementos de convicción, respetando el debido proceso y las garantías constitucionales y procesales, tales como Art. 226.- Interceptación e incautación postal, en el artículo 230 la intervención de comunicaciones y telecomunicaciones – Intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación.

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

En el Perú, los principios inspiradores que rigen la actuación del Juez al autorizar el uso de nuevas tecnologías en las investigaciones son:

1. Principio de Subsidiaridad: Se aplicarán solamente si no existen otros métodos de investigación convencional que posibiliten que el delito sea detectado o sus autores identificados.
2. Principio de Necesidad: Sólo se utilizarán atendiendo a los fines de la investigación en relación con la importancia del delito investigado.
3. Principio de Proporcionalidad: Se usarán sólo si la protección del interés público predomina sobre la protección del interés privado.
4. Principio de Especialidad: La información recolectada solamente podrá ser usada para probar la acusación que fue materia de la investigación. (Excepcionalmente puede ser utilizada para el esclarecimiento de otros delitos).
5. Principio de Reserva: Las actuaciones referidas a las técnicas especiales solo serán de conocimiento de los funcionarios autorizados por ley.

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

Sobre esta materia existe la Ley N° 27697 del 2002, "que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional". Con fundamento en ella, si se puede utilizar un micrófono como medida de investigación, siempre y cuando se encuentra autorizado con una resolución judicial, que permita la utilización de equipos electrónicos en la investigación, sin embargo, en la norma no se señala tácitamente el uso de esos equipos electrónicos, empero, para no vulnerar algún derecho fundamental, es por ello que se requiere una autorización mediante una resolución judicial.

¿Cómo valora la normativa interna de su país relativa a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos (celulares, tablets, computadoras...)?

Todo proceso respecto a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos dentro de un caso o proceso penal, son de suma reserva, y para ello, lo ampara nuestra Constitución Política del Perú y las normas procesales. Se estaría cometiendo un delito si estos fueran revelados, porque se estaría vulnerando o recortando nuestros derechos fundamentales.

¿Qué valor se otorga en su país a la prueba digital (e-evidence) obtenida por Comisión Rogatoria Internacional?

La conservación de datos informáticos en el Perú es considerada la medida que tiene como finalidad realizar el aseguramiento de datos de información que se encuentran almacenados en un sistema informático y respecto de los cuales, posteriormente se requerirá su revelación por la autoridad competente, con posterioridad. Se justifica por la alta volatibilidad de los datos informáticos.

¿Considera adecuada la legislación de su país sobre obligación de conservación de datos por las operadoras de comunicación para la investigación y prueba de los delitos?

Sí, estoy de acuerdo, porque para que la autoridad competente (Ministerio Publico), requiera esos tipos de datos, su requerimiento debe estar debidamente fundamentado, para que el Juez autorice mediante una resolución Judicial y estos no puedan ser vulnerados, como ha sido explicado en las repuestas de las preguntas del tema

En su país, ¿es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional?

En Perú, la Unidad de Cooperación Judicial Internacional y Extradiciones de la Fiscalía de la Nación en cumplimiento de las funciones establecidas en el artículo 512 del Código Procesal Penal, y en la Resolución de la Fiscalía de la Nación N° 124-2006-MP-FN, brinda lineamientos básicos para efectuar la conservación de datos en el marco de investigaciones de ciberdelincuencia, ya sea de manera directa mediante las plataformas en línea o mediante las redes internacionales; así como desarrolla los requisitos necesarios para la formulación de una solicitud de asistencia judicial internacional en esta materia.

Para ello se deben seguir los siguientes pasos:

1er Paso: Efectuar la conservación de los datos informáticos.

2do Paso: Requerir la información de abonado o de suscriptor.

3erPaso: Formular una solicitud de asistencia judicial internacional.

El Convenio de Budapest, vigente en el Perú, desde el 1 de diciembre de 2019, establece en el artículo 23, que la cooperación entre los países se realizará para las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de los delitos.

La medida se encuentra recogida en el artículo 29 de la Convención de Budapest, y establece que una parte podrá solicitar a otro Estado, parte que ordene la conservación rápida de datos almacenados por medio de sistemas informáticos que se en-

cuentren en dicho territorio y en relación con los cuales la parte requirente tenga la intención de presentar una solicitud judicial o que pueda obtener la revelación de dichos datos.

La Red 24/7 fue creada en virtud de lo establecido en el Convenio de Budapest y puede ser utilizada en los 65 Estados Parte entre ellos el Perú. Se requiere la designación de un punto de contacto localizable las 24 horas del día, los 7 días a la semana. En el caso peruano, el punto de contacto recae en la Autoridad Central. La Fiscalía de la Nación designó como puntos de contacto del Perú.

La Red de Crímenes de Alta Tecnología-Red G7, se encuentra reconocida por la Organización de Estados Americanos y actualmente puede ser utilizada en 90 Estados, los que en su mayoría no forman parte del Convenio de Budapest. Sin embargo, existe un grupo de países que además de formar parte del Convenio de Budapest, también forman parte de la Red G-7, tales como: Estados Unidos, Argentina, Chile, Perú, entre otros. En el caso peruano, las coordinaciones se realizan con la UCJIE, en su calidad de Autoridad Central en materia de cooperación jurídica internacional.

¿Tipifica su país bajo un título, capítulo, los ciberdelitos?

No informa.

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

La doctrina dominicana es prácticamente nula en el ámbito de derecho penal económico, solo se cuenta con escasos artículos publicados en revistas y periódicos desde el inicio de la República, y existían reglas que conformaban su derecho penal económico, tales como ciertos tipos de robos y estafas, falsedades como la monedas y de timbres o sellos del Estado, el soborno y el cohecho, la prevaricación y los delitos contra la libertad de subasta entre otras.

No obstante todo lo anterior, vale la pena destacar que frente al fenómeno de obtención de fondos y valores a través de constreñimiento señala la legislación penal lo siguiente:

Artículo 14.- Obtención Ilícita de Fondos. El hecho de obtener fondos, créditos o valores a través del constreñimiento del usuario legítimo de un servicio financiero informático, electrónico, telemático o de telecomunicaciones, se sancionará con la pena de tres a diez años de prisión y multa de cien a quinientas veces el salario mínimo.

Párrafo. - Transferencias Electrónica de Fondos. La realización de transferencias electrónicas de fondos a través de la utilización ilícita de códigos de acceso o de cualquier otro mecanismo similar, se castigará con la pena de uno a cinco años de prisión y multa de dos a doscientas veces el salario mínimo.

En realidad, una de las conductas más comunes, y que constituye la queja recurrente de usuarios de productos bancarios, es la clonación de tarjetas, pero por lo general en estos casos, el usuario denuncia poco a las autoridades, ya que la usanza es que es la institución financiera la que procura la apertura de las investigaciones al respecto. El cliente se conforma con una reclamación, y las instituciones bancarias ofertan seguros, como una forma de protección a los clientes.

De su lado la Ley núm. 155-17 contra el Lavado de Activos y el Financiamiento del Terrorismo tiene entre los delito Precedente o Determinante, para que pueda considerarse lavado de activos, los delitos de alta tecnología, lo que significa, que la utilización de la tecnología con fines de blanquear capitales también encuentra en esta ley una respuesta.

Por otra parte, la Estafa establecida en el Artículo 15: La estafa realizada a través del empleo de medios electrónicos, informáticos, telemáticos o de telecomunicaciones, se sancionará con la pena de tres meses a siete años de prisión y multa de diez a quinientas veces el salario mínimo.

Cuando la infracción establece los Delitos Relacionados a la Propiedad Intelectual y Afines. Cuando las infracciones establecidas en la Ley No.20-00, del 8 de mayo del año 2000, sobre Propiedad Industrial, y la Ley No.65-00, del 21 de agosto del año 2000, sobre Derecho de Autor, se cometan a través del empleo de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o de cualquiera de sus componentes, se sancionará con las penas establecidas en las respectivas legislaciones para estos actos ilícitos.

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

De manera congruente con lo antes expresado, la legislación dominicana no regula de manera expresa elementos propios de la ciberdelincuencia. Estas son conductas que se judicializan bajo otra denominación de otros tipos penales que se conocen en la legislación nuestra son reconocidas por nuestra legislación.

Los principales delitos electrónico en República Dominicana son jaquear cuentas como Twitter, Facebook, correo electrónico, intervenir llamadas de telefónicas.

Así mismo, se pueden incluir dentro de los mismos, atentados sexuales y pornografía infantil, y aunque de hecho existen todas las formas de ciberacoso como modalidad de ciberdelito intrusivo, son conductas que se judicializan bajo denominación de otros tipos penales que si son reconocidos por la legislación nacional.

En el Código Penal se recoge por ejemplo algunas formas de violencia contra la mujer debido a su género, articulo 309-1 y siguientes del Código Penal, el atentado voluntario contra la intimidad y la vida privada contenida en el artículo 337, la publicación de imágenes o montajes, y el acoso telefónico, contenida en el artículo 338, todos del Código Penal dominicano.

¿Tiene su legislación procesal penal medidas restrictivas de internet (bloqueo,

No, el artículo 54 otorga al Ministerio Público, previo cumplimiento de las formalidades dispuestas en el Código Procesal Penal, el Ministerio Público, quien podrá auxiliarse de una o más de las siguientes personas: organismos de investigación del Estado, tales como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional; la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de Investigaciones; peritos; instituciones públicas o privadas, u otra autoridad competente.

¿Cuáles son las medidas concretas de investigación con medios tecnológicos que contempla la legislación penal de su país?

Para el caso dominica, la legislación penal no contempla ninguna medida tecnológica de investigación criminal para perseguir los crímenes y delitos cibernéticos, pero en el año 2007 se creó la Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología, en dicha ley se crean organismos especializados en dicha materia.

Se creó la Fiscalía especializada para dicha aérea, así como la Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología (CICDAT), el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) y la División de Investigaciones de Delitos Informáticos (DIDI).

En complemento de lo anterior, el artículo 192 del Código Procesal Penal dominicano contempla el procedimiento para la interceptación de telecomunicaciones, y al respecto manda a que debe darse autorización judicial para la interceptación, captación, rastreo y grabación de las comunicaciones, mensajes de textos, datos, imágenes o sonidos transmitidos a través de redes públicas o privadas de telecomunicaciones por el imputado o cualquier otra persona que pueda facilitar razonablemente información relevante para la determinación de un hecho punible, cualquiera sea el medio técnico utilizado para conocerlas.

En estos casos manda a que se procesa conforme a las reglas del allanamiento. Refiere que tiene carácter excepcional y debe renovarse cada sesenta días, expresando los motivos que justifican la extensión del plazo, y que el funcionario encargado (siempre del ministerio público) debe levantar acta detallada de la transcripción de las comunicaciones útiles y relevantes para la investigación con exclusión de cualquier otra comunicación de carácter personal o familiar, (solo buscar lo que se necesita). Un punto relevante es que de acuerdo con esa norma la interceptación de comunicaciones sólo se aplica a la investigación de hechos punibles cuya sanción máxima prevista supere los cuatro años de privación de libertad y a los casos que se tramitan conforme el procedimiento especial para asuntos complejos.

Siempre a instancia o petición del ministerio público, y ordenada por el Juez de la instrucción, siempre que sea debidamente fundamentada.

¿Quiénes pueden solicitar y decretar estas medidas?

El Ministerio Público es quien solicita practicar cualquier diligencia que crea pertinente para la investigación de cualquier hecho ilícito, el juez es quien autoriza dichas actuaciones, si entiende que son pertinente.

¿Pueden los particulares y detectives o investigadores privados utilizar medidas tecnológicas de investigación sin autorización judicial y en qué supuestos?

No informa.

¿Existe en su país una normativa que regula específicamente las medidas de investigación tecnológica restrictivas de derechos fundamentales y cómo la valora?

No informa.

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

No informa.

¿Es necesario autorización judicial para colocar una baliza en su país? ¿Hay regulada la posibilidad de utilizar judicialmente otras herramientas de geolocalización? En caso afirmativo, explique brevemente los requisitos exigibles.

No informa.

¿Cómo valora la normativa interna de su país relativa a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos (celulares, tablets, computadoras...)?

No informa.

¿Qué obstáculos se encuentran cuando la autoridad judicial de su país ha de acceder a los datos de un proveedor de servicios que está situado en otro Estado?

No informa.

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización judicial? ¿Cuál? y ¿Por qué no la exige?

No informa.

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

No informa.

¿Qué valor se otorga en su país a la prueba digital (e-evidence) obtenida por Comisión Rogatoria Internacional?

No informa.

En su país, ¿es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional?

No informa.

¿Considera adecuada la legislación de su país sobre obligación de conservación de datos por las operadoras de comunicación para la investigación y prueba de los delitos?

No informa.

¿Tipifica su país bajo un título, capítulo, los ciberdelitos?

La República Oriental del Uruguay no tipifica en forma sistemática bajo un mismo título los delitos informáticos o ciber delitos.

Uruguay no ha ratificado aún el Convenio sobre Cibercriminalidad de Budapest de 23 de noviembre de 2001, ni el Convenio Iberoamericano de Cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelincuencia suscrito en Madrid en 2014, no obstante, ello en el presente año 2021 se han presentado informes en el parlamento afines a su pronta ratificación.

Por otra parte, la legislación uruguaya ha ido incorporando algunos ciber delitos en diversas leyes especiales, algunos de ellos son agregados al Código Penal y otros se mantienen en normas especiales, lo que hace que exista una diseminación importante en la normativa referente a esta temática. De la misma manera algunas modalidades de ciberdelitos que no se encuentran específicamente tipificados son abarcados por viejas pero vigentes figuras penales.

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

No informa

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

Actualmente en el país está vigente el artículo 92 de la ley 19580, ley de violencia de género, en donde se establece el delito de divulgación de imágenes o grabaciones con contenido intimo (sexting) conducta que se agrava en su artículo 93 en determinadas condiciones del sujeto pasivo sea su falta de consentimiento , minoridad , su capacidad o si la conducta fue con fin lucrativo.

Otro tema para considerar es la interceptación de las misivas estas constituyen delito lo cual se ve refrendado por la Ley 18.331 referentes a datos personales y habeas data, consagrando este derecho a rango de Derecho humano por cuanto nadie puede interrumpir el flujo y el control de datos.

Así mismo, lo concerniente a la penalización de la pornografía infantil. Fabricación, producción, comercio difusión, facilita miento de la comercialización y difusión de material pornográfico. (arts. 1, 2 y 3 ley 17815 de 6/9/2004).

Por otra parte, el Retiro o destrucción de medios o dispositivos electrónicos. (art. 359 Bis C.P., incorporado por ley 19889 de 24/7/2020. Y el artículo 277 bis del código penal que señala: "El que mediante la utilización de tecnologías, de internet, de cualquier sistema informático cualesquier medio de comunicación o tecnología de trasmisión de datos contactare a persona menor de edad o ejerza influencia sobre el mismo con el propósito de cometer cualquier delito contra su integridad sexual, actos con connotaciones sexuales, obtener

material pornográfico u obligarlo a hacer o no hacer algo den contra de su voluntad será castigado con de seis meses de prisión a cuatro años de penitenciaría" (incorporado al CP por art. 94 de ley 19580).

¿Tiene su legislación procesal penal medidas restrictivas de internet (bloqueo, retiro de páginas web, etc.) en materia de ciberdelincuencia económica e intrusiva?

No hay una legislación específica que permita adoptar medidas restrictivas, no obstante se dispone de otras herramientas genéricas que podrían ser adoptadas según el caso concreto.

Ejemplo de lo anterior es lo que ocurre en el marco de los delitos referentes a la propiedad intelectual donde se establece algunas medidas específicas con fundamento en la Ley 9739 modificada por Ley 17616 en el art. 48

¿Pueden los particulares y detectives o investigadores privados utilizar medidas tecnológicas de investigación sin autorización judicial y en qué supuestos?

No existe un supuesto legal en que se puedan utilizar medidas tecnológicas de investigación sin autorización judicial.

¿Cuáles son las medidas concretas de investigación con medios tecnológicos que contempla la legislación penal de su país?

En Uruguay se contempla como medios tecnológicos la interceptación de llamadas telefónicas, whatsapp y correo electrónico, solicitud que debe establecer en forma precisa el hecho de investigación datos de identificación del sujeto, número telefónico en caso de escucha y en este precisamente, si necesita el historial a los efectos de marcar una ruta o solo audios. Al igual que la disertación el juez, debe realizar ese control de legalidad, si algún elemento falta la orden debe rechazarse y ser enviada nuevamente. Sin perjuicio además de poder realizar actividades de video vigilancia (Árt. 210)

Por otra parte, en el marco de la Ley 19574 referente a lavado de activos se prevé el art. 62 que establece la posibilidad de vigilancia electrónica, concretamente en la investigación de cualquiera de los delitos previstos en los artículos 30 a 33 de la citada ley, así como de las actividades delictivas precedentes establecidas en el artículo 34 del mismo cuerpo normativo. En esos eventos se podrán utilizar todos los medios tecnológicos disponibles a fin de facilitar su esclarecimiento.

La ejecución de las vigilancias electrónicas será ordenada por el tribunal de la investigación a requerimiento del Ministerio Público. El desarrollo y la colección de la prueba deberán verificarse bajo la supervisión del tribunal penal competente. El tribunal penal competente será el encargado de la selección del material destinado a ser

utilizado en la causa y la del que descartará por no referirse al objeto probatorio.

El resultado de las pruebas deberá transcribirse en actas certificadas a fin de que puedan ser incorporadas al proceso y el tribunal está obligado a la conservación y custodia de los soportes electrónicos que las contienen, hasta el cumplimiento de la condena.

Una vez designada la defensa del intimado, las actuaciones procesales serán puestas a disposición de la misma para su control y análisis, debiéndose someter el material al indagado para el reconocimiento de voces e imágenes.

Quedan expresamente excluidas del objeto de estas medidas las comunicaciones que mantenga el indagado con su defensor, en el ejercicio del derecho de defensa y las que versen sobre cuestiones que no tengan relación con el objeto de la investigación.

La Unidad Reguladora de Servicios de Comunicaciones podrá aplicar las sanciones enumeradas en el artículo 89 de la Ley N° 17.296, de 21 de febrero de 2001, a aquellos operadores de servicios de telecomunicaciones que dificulten o impidan la ejecución de este tipo de vigilancias, dispuestas por la justicia competente."

¿Qué principios inspiradores rigen la actuación del Juez cuando autoriza la investigación criminal a través del uso de nuevas tecnologías?

No informa.

¿Existe en su país una normativa que regula específicamente las medidas de investigación tecnológica restrictivas de derechos fundamentales y cómo la valora?

En Uruguay se ha generalizado y reglamentado el uso de medios tecnológicos para la investigación de hechos con apariencia delictiva principalmente la interceptación de llamadas whatsaap y demás datos correos electrónicos etc. Para lo cual, se necesita petición por parte del Ministerio Publico y ser aprobados por juez competente, quien es el Juez de Garantías en el proceso y que llevara el referido hasta el momento del juicio.

¿Hay alguna medida tecnológica de investigación que se pueda usar y tenga validez probatoria en su sistema legal que no necesite de autorización judicial? ¿Cuál? y ¿Por qué no la exige?

El artículo 210 del CPP prevé que la videovigilancia se realice con noticia al juez, sin conocimiento del afectado; la misma debe realizarse en lugares expuestos al públicos o lugares abiertos, y habilita a tomar fotografías, registro de imágenes u otros medios técnicos especiales.

El presupuesto ineludible es que el juez este enterado de tal situación. En ese sentido señala la norma:

Videovigilancia Artículo 210. (Presupuesto y Ejecución).
210.1 El fiscal con noticia al juez y sin conocimiento del afectado, puede ordenar:

a) realizar tomas fotográficas y registro de imágenes; b) utilizar otros medios técnicos especiales en lugares abiertos expuestos al público.
210.2 Se requerirá autorización judicial cuando dichas actividades se realicen en el interior de inmuebles o lugares cerrados.

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

En estos dos puntos considero que se puede utilizar un micrófono como medida de investigación en virtud de que el art. 208 antes descripto refiere a intervención, grabaciones o registro de comunicaciones telefónicas u otras formas de comunicación, por lo que cuando hablamos otras formas de comunicación se autoriza la que se realiza en forma presencial y directa.

Los requisitos refieren a probar que se cometió un ilícito, que el indagado ha sido copartícipe del mismo de alguna forma, que la medida es necesaria y los motivos por los cuales es necesaria, que los hechos investigados revisten gravedad tal que habilita la limitación del derecho.

¿Es necesario autorización judicial para colocar una baliza en su país? ¿Hay regulada la posibilidad de utilizar judicialmente otras herramientas de geolocalización? En caso afirmativo,

No informa

¿Tienen habilitación legal para poder utilizar un micrófono como medida de investigación? En caso afirmativo, especifique brevemente las normas y los requisitos exigibles.

En estos dos puntos considero que se puede utilizar un micrófono como medida de investigación en virtud de que el art. 208 antes descripto refiere a intervención, grabaciones o registro de comunicaciones telefónicas u otras formas de comunicación, por lo que cuando hablamos otras formas de comunicación se autoriza la que se realiza en forma presencial y directa.

Los requisitos refieren a probar que se cometió un ilícito, que el indagado ha sido copartícipe del mismo de alguna forma, que la medida es necesaria y los motivos por los cuales es necesaria, que los hechos investigados revisten gravedad tal que habilita la limitación del derecho.

¿Cómo valora la normativa interna de su país relativa a la custodia y preservación de los datos obtenidos en el registro de dispositivos electrónicos (celulares, tablets, computadoras...)?

No informa

¿Qué obstáculos se encuentran cuando la autoridad judicial de su país ha de acceder a los datos de un proveedor de servicios que está situado en otro Estado?

No informa

¿Qué valor se otorga en su país a la prueba digital (e-evidence) obtenida por Comisión Rogatoria Internacional?

No informa

En su país, ¿es posible que la autoridad judicial se dirija directamente al proveedor de servicios situado fuera del territorio nacional?

No informa

¿Considera adecuada la legislación de su país sobre obligación de

Los datos solo se mantienen en todo el proceso, es decir hasta la casación respectiva como derecho de todo reo, una vez que la sentencia fuera confirmada esos datos deben restituirse o destruirse, siendo adecuada en mi país la normativa haciendo honor a los principios proporción, especialidad y necesariedad, es decir que sea el único medio de prueba eficaz.

Consejo General del Poder Judicial

Aula Iberoamericana
Consejo General del Poder Judicial

Cooperación Española
CONOCIMIENTO / INTERCOONECTA

SISTEMATIZACIÓN DEL CURSO VIRTUAL

CURSO LA CIBERDELINCUENCIA: TRATAMIENTO PREVENTIVO, PROCESAL Y SUSTANTIVO DESDE UNA PERSPECTIVA INTERNACIONAL

2021