SISTEMATIZACIÓN DEL CURSO VIRTUAL

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

Del 23 de noviembre al 4 de diciembre de 2020
Cartagena de Indias

Consejo General del Poder Judicial

Aula Iberoamericana
Consejo General del Poder Judicial

Cooperación Española
CONOCIMIENTO / INTERCOONECTA

CONTENIDO

...Este espacio de intercambio de saberes permitió conocer 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 como la intimidad, el secreto profesional, el patrimonio económico, la libertad, integridad y formación sexual...

Inauguración del Curso virtual LA CIBERDELINCUENCIA: TRATAMIENTO PREVENTIVO, PROCESAL Y SUSTANTIVO DESDE UNA PERSPECTIVA INTERNACIONAL

...un espacio de reflexión y debate dirigido a diferentes profesionales en Derecho...

Del 23 de noviembre al 4 de diciembre de 2020 el Centro de Formación de la Cooperación Española en Cartagena de Indias desarrolló el Curso virtual *'La ciberdelincuencia: tratamiento preventivo, procesal y sustantivo desde una perspectiva internacional'*, un espacio de reflexión y debate dirigido a diferentes profesionales en Derecho de países como Colombia, Argentina, Brasil, Perú, Chile, Nicaragua, Guatemala, El Salvador, Panamá, Uruguay, Paraguay, Cuba, República Dominicana, Costa Rica, Ecuador y Honduras.

Las temáticas en materia de normatividad, dogmática y tratamiento procesal en el contexto de la ciberdelincuencia fueron abordados por el coordinador del curso, Alberto Varona Jiménez, Magistrado de la Audiencia Provincial de Barcelona, profesor de Derecho penal y Procesal penal de la Escuela Judicial de Consejo General del Poder Judicial de España y por Eloy Velasco Núñez, Magistrado de la Sala de Apelaciones de la Audiencia Nacional y Joaquín Delgado Martín, Magistrado de la Audiencia Provincial de Madrid.

Este espacio de intercambio de saberes permitió conocer 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 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. 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.

Las jornadas de este curso permitieron llegar a heterogéneos hallazgos, conclusiones y recomendaciones, los cuales abordaremos en dos apartados. 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. 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.

1

CIBERDELINCUENCIA: Tratamiento sustantivo y procesal.

...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...

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. Por otra parte, con el desarrollo de las tecnologías de la información y la comunicación, así como de la Internet a finales del siglo XX, le imprimieron velocidad a estos cambios hasta el punto 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 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 (TICS), son una combinación de medios informáticos con medios de comunicación y comprenden: Sistemas Informáticos, Redes Sociales, ordenadores, foros virtuales, etc. Las TICS han adquirido un desarrollo y han generado una

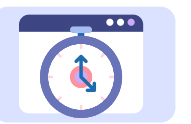
[1] Unidad mínima de información.

necesidad abrumadora a partir de la entrada en vigencia 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 TICS, 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 TICS forma parte de una evolución cuyo ritmo se aceleró a finales de la década del cincuenta 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 e1967 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. Así mismo, en el año de 1969 se va a dar 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:

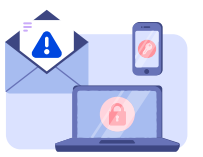
Anonimato: Delitos cometidos a distancia, sin posible reacción inmediata de la víctima.



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 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:

CRITERIOS FUNDAMENTALES

- **Armonizar las leyes nacionales**
- **Mejorar las técnicas de información en este tipo de delitos**
- **Aumentar la cooperación entre naciones**
- **Establecer principios para dirimir aspectos procesales en los que se ventilen estas conductas.**

El convenio de Budapest ha sido ratificado por 65 países, además de multitud de Estados de Europa y de otras regiones (EEUU, 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

CIBERDELINCUENCIA ECONÓMICA

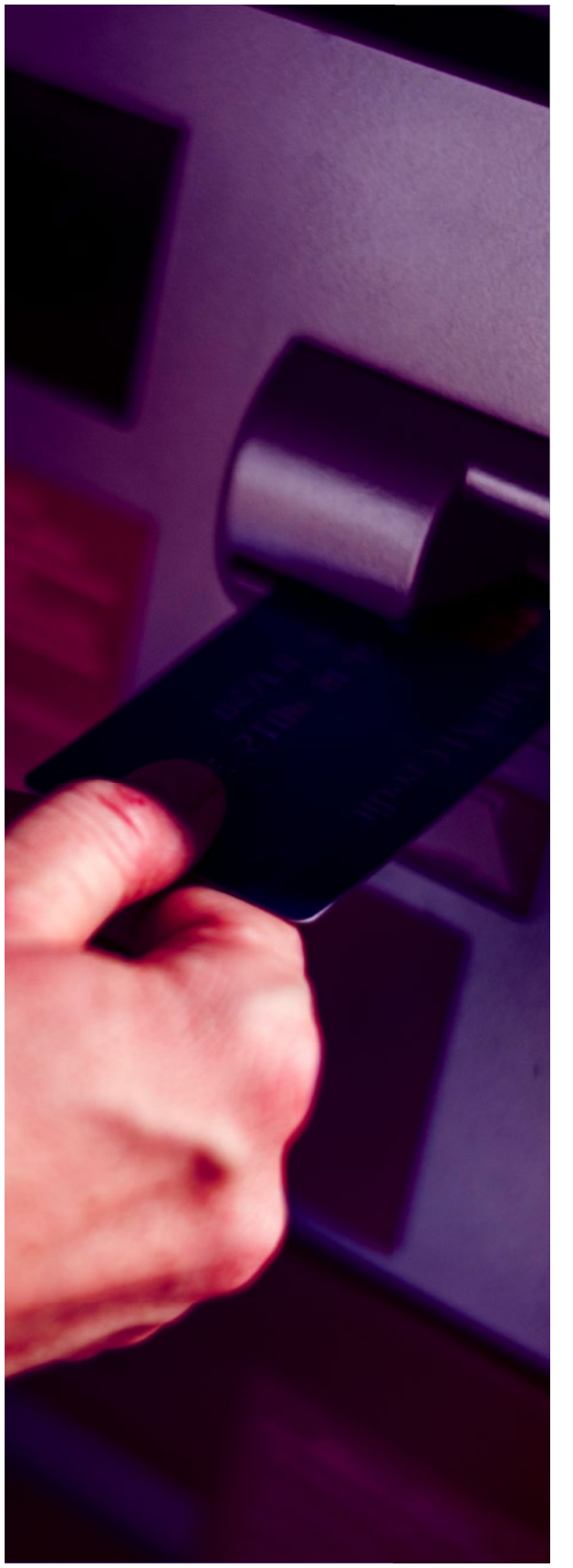
...La ciberdelincuencia económica se caracteriza fundamentalmente porque el delincuente, mediante el uso de dispositivos y tecnologías informáticas, se apodera de dineros y activos ajenos para su beneficio lucrativo o de un tercero...

Durante este espacio se abordó el estudio dogmático de los comportamientos que configuran ciberdelitos. Desde esa visión, se planteó que los ciberdelitos pueden ser clasificados de la siguiente manera: Ciberdelincuencia Económica, Ciberdelincuencia Intrusiva y Ciber Espionaje-Ciber Terrorismo.

La 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. El Código Penal español[2] 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. 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 TICS. Su preparación, ejecución y consumación se hace por medios informáticos. Como ejemplo podemos citar: las Cartas Nigerianas[3] , el Phishing[4] , 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 objeti-



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

[3] 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.

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

vo 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 Numero de Dominio (DNS) para obtener claves e información de las víctimas enviándolas a páginas web distinta a la que quiere acceder el usuario. 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.

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[5]; (ii) también se penaliza a quien interrumpa u obstaculice el sistema informático ajeno sin estar autorizado para ello, conocido como Denial of Service[6]. 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

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

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

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 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".

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 frentes 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, trafico 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

CIBERDELINCUENCIA INTRUSIVA

Los delitos ciber-intrusivos son aquellos en los cuales el delincuente busca fundamentalmente obtener información y datos de la vida íntima y privada -principalmente sexuales- de terceras personas mediante el uso malicioso de las TICS. Como ejemplos de este tipo de delitos tenemos: la Pornografía Infantil, articulo 189 Código Penal español, el Abuso Sexual, artículo 183 bis, el Child Grooming, artículo 183 ter del código penal, el Descubrimiento y Revelación de Secretos, artículo 197 del Código Penal.

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. Para la configuración de 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 TICS. 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 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[7], Spyware[8] , Keyloggers[9] , Botnest[10] , virus[11] - busca descubrir los secretos o vulnerar la intimidad de una persona, se apodera de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos 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 TICS, como instrumentos para perpetrar delitos considerados tradicionales en materia penal, como son la Injuria y la Calumnia, tipificados en los artículos 205 y 208 del Código Penal español.

---

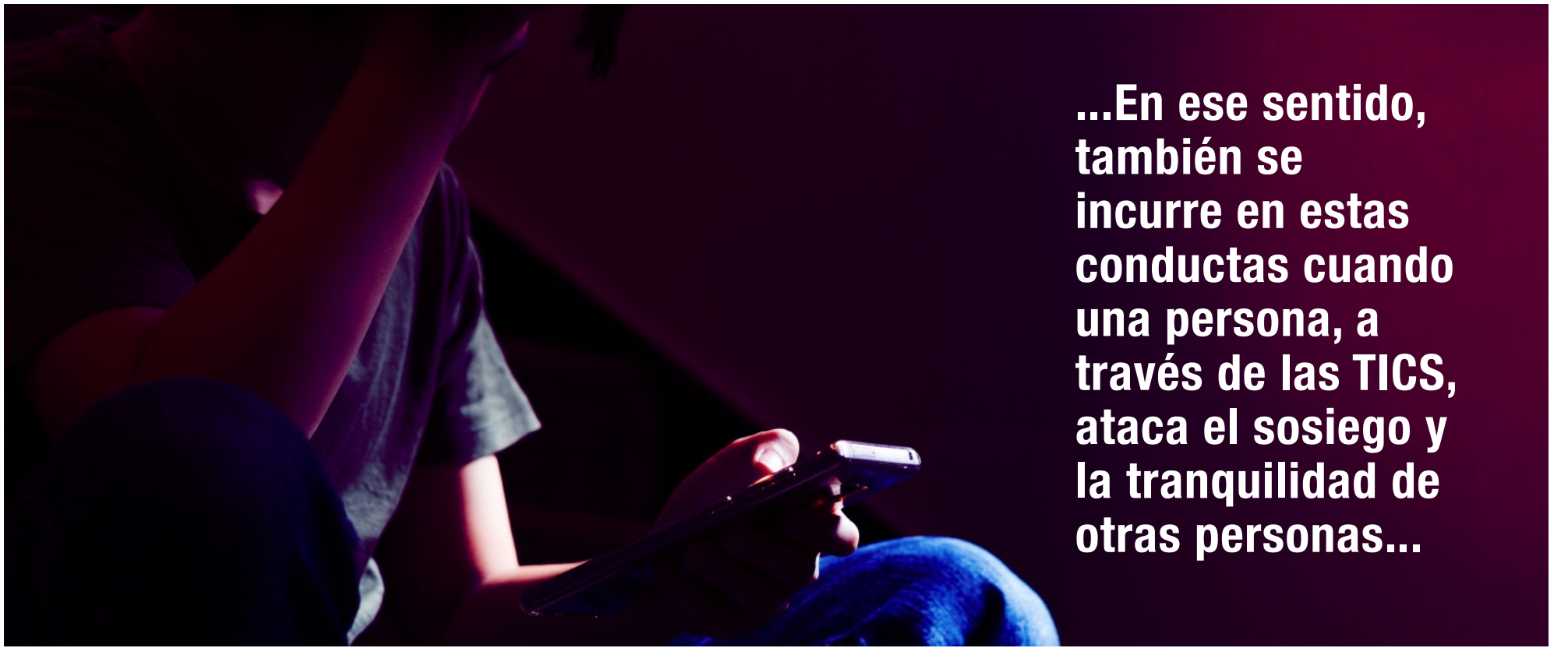
[7] Malware (Software malicioso) que se presente al usuario como legítimo, pero que, al ser utilizado por el usuario, le permite al hacker o al delincuente un acceso desde la distancia, al equipo infectado.

[8] 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.

[9] 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.

[10] 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.

[11] 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.



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 TICS, 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 TICS 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[12] - en sus mensajes extorsionadores y le exigen un pago en dinero -al usuario- para no denunciarlo o exponerlo.

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

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.

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.

1.3

LA CIBERDELINCUENCIA: ASPECTOS PROCESALES, FUENTES DE LA PRUEBA DIGITAL Y MECANISMOS DE COOPERACIÓN INTERNACIONAL.

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[13] , Legalidad[14] , Especialidad[15] , Necesidad-Excepcionalidad[16] , Idoneidad[17] y de Proporcionalidad[18] . 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

...la regla general es que ninguna persona puede estar contantemente vigilada e interceptada por organismos del Estado...

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.

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

...Cada fuente de la prueba digital u origen de la prueba digital tiene una institución procesal...

Enjuiciamiento Criminal permiten la utilización de dispositivos de seguimiento y de geolocalización.

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 este punto se hace necesario analizar algunas de las instituciones de investigación en materias telemáticas con fines judiciales, tal y como se abordaron en el curso sobre Ciberdelincuencia de manera sucinta para entender la importancia de estos medios. 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. Enel 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 Interceptación 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.

Como mencionábamos, en el curso sobre Ciberdelincuencia, también se estudió la institución de los Registros como medio de investigación, los cuales pueden recaer: (i) sobre Dispositivos electrónicos[19] ,(ii) Datos en la nube y (iii) Registros Remotos. En cada una de estas modalidades, 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: 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. Eel 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.

Por cualquier delito siempre que materialice el principio de proporcionalidad también puede darse de manera excepcional que sin autorización judicial, en situaciones de urgencia[20] y necesidad[21], la autoridad policial judicial acceda al dispositivo siempre cumpliendo el principio de proporcionalidad[22] 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. 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.

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

---

[19] 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.

[20] 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.

[21] 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.

[22] 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.

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.

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, Armazón, 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

...Con relación a los motores de búsqueda y sitios web no necesitan autorización judicial para acceder a esos datos...

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[23] 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.

En el ordenamiento jurídico español existe la figura del ciber patrullaje. El policía puede investigar apoyado en las Redes Sociales[24] , 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.

---

[23] 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.

[24] 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.

1.3.1 Dimensión Transnacional de la Prueba Digital

...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...

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 esta solo se puede articular a partir de un convenio bilateral. Sin embargo, estos convenios por lo general no consagran normas específicas sobre prueba digital, aunque es posible destacar varios convenios bilaterales 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 año001, que nace en el seno del Consejo de Europa, ha trascendido los limites 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[25] , Remisión[26] , acceso transfronterizo de Datos[27] .

---

[25] 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.

[26] 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.

[27] 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 informáticos almacenados en otro lugar, si la parte obtiene el consentimiento licito y voluntario de la persona legalmente autorizada para revelar los datos a la parte, por medio de ese sistema informático.

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 ratificado por Cuba, Nicaragua, Costa Rica, Perú, Uruguay y otros. 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.

Medidas de Aseguramiento

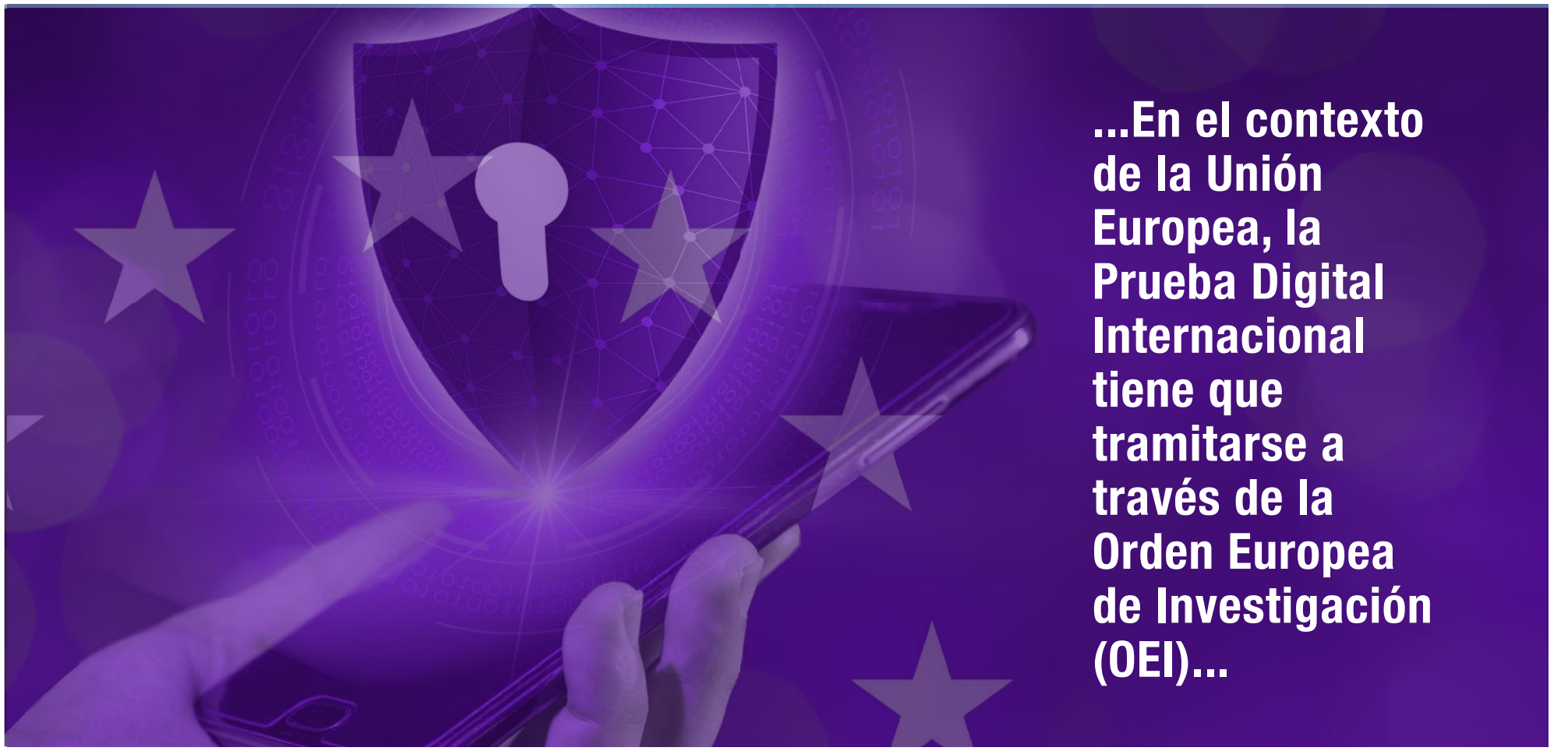
En el ámbito de Medidas de Aseguramiento el presente tratado regula lo siguiente:

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.

Diligencias de investigación

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)...

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 sobre Ciberdelincuencia 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.

2

CONCLUSIONES Y RECOMENDACIONES

Conclusiones y Recomendaciones

1. En la mayoría de las legislaciones penales de los países participantes -exceptuando algunos como Colombia o Guatemala- no existe un título en el cual se agrupe de manera sistemática los principales Ciberdelitos. Por el contrario, 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. Se hace necesario actualizar las diferentes legislaciones penales con las descripciones típicas que configuran los ciberdelitos de mayor ocurrencia y que no se contemplan en el derecho interno de los países participantes, así como la creación en los códigos penales de títulos específicos en los cuales se consagren los ciberdelitos de mayor ocurrencia, los más lesivos y graves, teniendo en cuenta la normatividad internacional en la materia, específicamente el Convenio de Budapest del 23 de noviembre de 2001.

2. En materia de Ciberdelincuencia Económica o Intrusiva se recomienda que, al igual que en España, los países latinoamericanos establezcan y desarrollen en sus legislaciones internas la figura del Agente Encubierto Virtual, toda vez que, en la mayoría de los casos, los delitos cibernéticos son perpetrados por organizaciones criminales.

3. Lo anterior hace necesario que, para contrarrestar la Ciberdelincuencia como fenómeno criminal transfronterizo, el Derecho Penal también vaya articulándose en red por medio de los mecanismos de Cooperación Penal Internacional.

4. En materia procesal los países latinoamericanos han ratificado en sus legislaciones penales procedimentales el Convenio de Budapest o el Tratado de Madrid.

5. Es necesario fortalecer la regulación de la cadena de custodia de la evidencia electrónica y de los datos informáticos de una manera acorde con el desafío que nos plantean las TIC, con el fin de proteger derechos fundamentales y fortalecer la investigación y el proceso penal.

6. Se requiere que las escuelas de formación judicial, las universidades y la Ciencia del Derecho Penal capaciten a sus funcionarios, formen a sus estudiantes y generen investigaciones científicas en materia de ciberdelincuencia pues, a pesar de que las TICS forman parte de nuestra vida cotidiana, para efectos forenses se carece de una formación informática básica que le permita al operador judicial desenvolverse en una situación concreta que involucre un ciberdelito, ya sea económico o intrusivo.

7. Como la Ciberdelincuencia trasciende las fronteras de Estado-Nación, se necesita que entre los países se generen mecanismos de cooperación internacional para perseguir de manera eficaz este tipo de criminalidad. Es importante entonces que se torne eficaz el acceso a los datos que se encuentran en proveedores de datos, ya sea fortaleciendo los convenios existentes sobre Prueba Digital Internacional o creando otros que permitan generar una relación directa de la autoridad judicial con el proveedor de servicios localizado en otro Estado.

8. 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.

9. Es necesario complementar la normativa internacional con reglamentaciones que nos permitan producir, obtener y asegurar la evidencia electrónica transfronteriza para que las investigaciones y el proceso penal sea eficaz.

10. Teniendo en cuenta que las medidas de investigación con medios tecnológicos puede llegar a ser invasiva y a lesionar derechos fundamentales, debe ser siempre un juez el que decida -ya sea juez de Instrucción o de Garantías- si decreta o no la medida. Y esta decisión debe ir debidamente fundamentada y motivada, cumpliendo siempre los principios de Legalidad, Necesidad, Idoneidad, Especialidad y Proporcionalidad.

3

FICHA POR PAIS: CIBERDELINCUENCIA

Argentina

¿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.

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

No informa

¿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 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.

¿Quiénes puedesn solicitar y decretar estas medidas?

Las solicita el Fiscal y las decreta el Juez. Pero solo la Interceptación Telefonica, las demas estan sujetos al principio de libertad probatoria.

Normatividad que en su país regula la investigación tecnológica restrictiva de Derechos Fundamentales

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

¿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

Brasil

¿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?

Por regla general las decreta el poder judicial, excepcionalmente la policia puede hacerlas directamente

Normatividad que en su país regula la investigación tecnológica restrictiva de Derechos Fundamentales

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

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

La ley brasileña contempla varias medidas específicas de investigación criminal tecnológica, siendo, por regla general, autorizadas por el Poder Judicial (hay excepciones, en las que la policía puede realizarlas directamente). Las personas y los detectives o investigadores privados no pueden, por regla general, utilizar medidas de investigación tecnológica sin autorización judicial.

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.

Como podemos ver a continuación, existen medidas tecnológicas de investigación que pueden ser utilizadas y tienen validez probatoria sin depender de autorización judicial:Art. 13-B. De ser necesario para la prevención y represión de delitos relacionados con

Brasil

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

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)

¿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

Chile

¿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?

El Fiscal

¿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 por cierto 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 formula 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.

Normatividad que en su país regula la investigación tecnológica restrictiva de Derechos Fundamentales

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.

¿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

Colombia

¿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 económicos que contempla su legislación?

Artículo 269 I, de la ley 599 del 2000, Hurto por medios informaticos y semejantes. Artículo 269 J, Transferencia no consentida de activos

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

Pornografia con personas menores de 18 años, artículo 218, ley 599 del 2000. Acceso Abusivo a un Sistema Informatico, Obstaculización ilegitima de sistema informaticos o red de telecomunicaciones, interceptación de datos informaticos, violación de datos personales, suplamtación de sitios web para capturar datos personales, Uso de Software malicioso, Daño informatico.

¿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 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.

¿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?

Algunas las puede ordenar el fiscal sin autorización, otras si requieren autorización del juez de control de garatías

Normatividad que en su país regula la investigación tecnológica restrictiva de Derechos Fundamentales

El precepto que regula la las medidas de investigacion tecnologica es la busqueda selectiva en base de datos, regulada en el art.244 del C. P.P, ley 906del 2004.

¿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?

Con respecto a esta pregunta, se considera que la regulacion al respecto es adecuada a los fines constitucionales y legales de la investigacion penal dado que las empresas de telecomunicacion cumplen de manera generica con el suministro de la informacion requerida.

Costa Rica

¿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

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

La investigación se rige por lo dispuesto en el Código Procesal Penal y en la Ley número 7425, que se denomina "Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones". Además, existen disposiciones en leyes tales como la Ley contra la Delincuencia Organizada, número 8754, en la que se creó el Centro Judicial de Intervención de las Comunicaciones (artículo 14), cuyo fin es centralizar la medida en un grupo de jueces y técnicos que se dediquen solo a dicha labor. Si bien no existe mayor referencia en la legislación, cualquier medida tecnológica de investigación que invada los derechos fundamentales de la persona imputada (o sobre quien recae la sospecha fundada) deberá ser ordenada por el Juez únicamente.

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

No informa

Normatividad que en su país regula la investigación tecnológica restrictiva de Derechos Fundamentales

No informa

¿Quiénes pueden solicitar y decretar estas medidas?

Si se trata de medidas tecnológicas que no implican una violación a un derecho fundamental (por ejemplo,

¿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

Cuba

¿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 tematica es nueva por lo cual, desde desde lo sustantivo y procesal no tienen hay tipificación, así como medios tecnológicos investigativos.

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

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

Normatividad que en su país regula la investigación tecnológica restrictiva de Derechos Fundamentales

No informa

¿Quiénes pueden solicitar y decretar estas medidas?

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

Ecuador

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

No existe un tratamiento sistematico en un título o en un capítulo de los ciber-delitos. Lo que existe son algunos tipos penales, del Código Orgánico Integral Penal. Trata únicamente ciertos delitos informáticos, como el Art. 190 que tipifica la apropiación fraudulenta por medios electrónicos. En igual sentido el Art. 232 trata sobre el ataque a la integridad de sistemas informáticos, agregando que, la dosificación punitiva es más alta, si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana. De su parte, el Art. 476 ibídem, prevé el tipo de interceptación de las comunicaciones o datos informáticos.

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

Art. 190 del Código Orgánico Integral Penal que tipifica la apropiación fraudulenta por medios electrónicos

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

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).

¿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.

¿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

Ecuador

¿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?

De acuerdo a 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 Fiscalía pueda investigar el cometimiento de una infracción.

Normatividad que en su país regula la investigación tecnológica restrictiva de Derechos Fundamentales

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 ibídem, 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.

El Salvador

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

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 los ciberdelitos económicos que contempla su legislación?

No informa

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

No informa

¿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.

¿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.

Normatividad que en su país regula la investigación tecnológica restrictiva de Derechos Fundamentales

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 ha de 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.

¿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.

Guatemala

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

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 los ciberdelitos económicos que contempla su legislación?

No informa

Normatividad que en su país regula la investigación tecnológica restrictiva de Derechos Fundamentales

Ley contra la Delicuencua Organizada

¿Quiénes pueden solicitar y decretar estas medidas?

Se indica que las puede solictar el minestrio público, pero no indica quién es el funcinario encargado de decretarla.

¿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, es adecuado.

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

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.

¿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 partre, 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).

Honduras

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

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 los ciberdelitos económicos que contempla su legislación?

No informa

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

No informa

¿Quiénes pueden solicitar y decretar estas medidas?

Las intervenciones telefonicas las solicita el fiscal y las decreta el Juez de Control de Grantias

¿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 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, Intercepta-ción 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.

¿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 OBLIGACION DE GUARDAR INFORMACION 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 termino de prescripción de delitos graves.

Honduras

Normatividad que en su país regula la investigación tecnológica restrictiva de Derechos Fundamentales

En Honduras mediante Decreto No. 243-2011 de fecha 8 de diciembre de 2011 se promulgó la 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 as 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.

Nicaragua

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

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 los ciberdelitos económicos que contempla su legislación?

No informa

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

No informa

Normatividad que en su país regula la investigación tecnológica restrictiva de Derechos Fundamentales

Nuestra 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.

¿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;

¿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 cuando 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.

¿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.

Panamá

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

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 los ciberdelitos económicos que contempla su legislación?

No informa

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

No informa

¿Quiénes pueden solicitar y decretar estas medidas?

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

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

1) Aprehensión Provisional de medios informáticos procedentes o relacionados al delito

Aprehensión Provisional de Bienes
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:

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.

Panamá

3) Incautación de Datos Informáticos

Artículo 314. Incautación de datos. Cuando se incauten equipos informáticos o datos almacenados en cualquier otro soporte, regirán las mismas limitaciones referidas al secretoprofesional 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 propias del Debido Proceso.

Panamá

¿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 MOVIL, 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

Normatividad que en su país regula la investigación tecnológica restrictiva de Derechos Fundamentales

El Código Procesal Penal de Panamá estable 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 MOVIL y TIGO (Anteriormente MOVISTAR), lo anterior con base en la Ley51 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.

Paraguay

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

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 los ciberdelitos económicos que contempla su legislación?

No informa

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

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 legisla para obtención de información que conlleve a llegar a la verdad real sobre los ciberdelitos y siempre bajo el pedido del órgano investigador que es el Ministerio Publico y bajo el control jurisdiccional del Juez Penal de Garantías, bajo 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.

Art. 200. Intervención de Comunicaciones.

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 quela 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, así lo dispone el art. 199 C.P.P.

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?

La solicita el Minestrio Público y la decreta el Juez de Control de Garantis

¿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.

Paraguay

Normatividad que en su país regula la investigación tecnológica restrictiva de Derechos Fundamentales

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 tenemos normativa específica pues no todas las medidas se encuentran previstas, si bien está en estudio por la Comisión de Reforma Penal. Los artículos 172 (búsqueda de la verdad); 173 (libertad probatoria) y 175 (exclusiones probatorias) son las utilizadas para fundamental los pedidos de exclusión de aquellos actos que no reúnan los requisitos exigidos.

Perú

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

En Perú está regulado en

¿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 los ciberdelitos económicos que contempla su legislación?

No informa

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

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?

Son adecudas

¿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 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.

¿Quién las puede solicitar y quién acordar o autorizar?

Las puede solicitar el Ministerio Público. En Honduras se ha nombrado un juez de garantías que conoce exclusivamente de las solicitudes para la intervención telefónica

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

No pueden es una competencia exclusiva del Ministerio Público, y solo pueden autorizarse mediante autorización de un juez de garantías en la investigación, persecución, y el procesamiento de los delitos en que se requiera la utilización de esta técnica especial, valorando para ello la gravedad, utilidad y proporcionalidad de la medida en relación al delito que se trate,

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

La ley se rige por los principios de proporcionalidad, necesidad, idoneidad, confidencialidad, reserva jurisdiccional, temporalidad

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

No, todas necesitan de autorización judicial porque son esencialmente restrictivas de derechos fundamentales,

FORO GENERAL - MODULO 3 - TECNICAS DE INVESTIGACION EN PERU

de María del Carmen Victoria Ruiz - domingo, 29 de noviembre de 2020, 09:52

Número de respuestas: 3

Imagen de PERÚ

1.- Cuáles son las concretas medidas tecnológicas de investigación criminal que contempla su sistema legal, su Código Procesal Penal?

Perú

El Código Procesal Peruano aprobado por Decreto Legislativo 957 del 29.07.2004, 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. Entre las medidas principales tenemos:

1.1.- La Videovigilancia ordenada por el Fiscal de oficio o a pedido de la Policía, se requiere de autorización judicial cuando es realizada en lugares cerrados o al interior de un inmueble.

1.2.- El allanamiento y registro domiciliario, la incautación con registro y detención de personas, la exhibición forzada e incautación en sus Artículos 214, 217 y 218, Control de comunicaciones y documentos privados – 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. Artículo 231.- Registro de la intervención de comunicaciones telefónicas o de otras formas de comunicación, Artículo 232.- Aseguramiento e incautación de documento privado que no tenía orden de incautación, Art. 235.- El levantamiento del secreto bancario, reserva tributaria, Artículo 237.- Clausura o vigilancia de locales e inmovilización.

1.3.- Asimismo se ha regulado las medidas de coerción procesal de restricción de derechos fundamental con expresa autorización judicial y con respeto al principio de proporcionalidad, necesidad, idoneidad, racionalidad, y que existan suficientes elementos de convicción, tales como la detención preliminar, la prisión preventiva, así como prevé la suspensión preventiva de derechos y otras medidas reales como medidas anticipativas (art. 312), medidas preventivas y cautelares contra personas jurídicas, y la Incautación.

1.4.- Los actos especiales de investigación como: Art. 340.- Circulación y entrega vigilada de bienes delictivos, Art. 341.- Agente encubierto y agente especial y Art. 341-A.- Operaciones encubiertas.

1.5.- También se ha regulado en la Ley 30077 Medidas coercitivas y técnicas especiales de Investigación en el marco de la Ley de Crimen Organizado, que comprende:

Artículo 8. Interceptación postal e intervención de las comunicaciones. En el ámbito de la presente Ley, se respetan los plazos de duración de las técnicas

Perú

especiales de interceptación postal e intervención de las comunicaciones previstas en el inciso 2 del artículo 226 y en el inciso 6 del artículo 230 del Código Procesal Penal aprobado por Decreto Legislativo 957, respectivamente. 2. El trámite y realización de estas medidas tienen carácter reservado e inmediato.

Artículo 9. Interceptación postal 1. Solo se intercepta, retiene e incauta la correspondencia vinculada al delito objeto de investigación vinculado a la organización criminal, procurando, en la medida de lo posible, no afectar la correspondencia de terceros no involucrados.

Artículo 10. Intervención de las comunicaciones, Artículo 13. Agente encubierto, Artículo 14. Acciones de seguimiento y vigilancia.

Artículo 15. Deber de colaboración y de confi dencialidad de las instituciones y entidades públicas y privadas 1. Todas las instituciones y organismos del Estado, funcionarios y servidores públicos, así como las personas naturales o jurídicas del sector privado están obligadas a prestar su colaboración cuando les sea requerida para el esclarecimiento de los delitos regulados por la presente Ley, a fi n de lograr la eficaz y oportuna realización de las técnicas de investigación previstas en este capítulo.

2. La información obtenida como consecuencia de las técnicas previstas en el presente capítulo debe ser utilizada exclusivamente en la investigación correspondiente, debiéndose guardar la más estricta confidencialidad respecto de terceros durante y después del proceso penal, salvo en los casos de presunción de otros

Incautación y Decomiso

Atículo 17. Procedencia En todas las investigaciones y procesos penales por delitos cometidos a través de una organización criminal, según lo previsto por la presente Ley, la Policía Nacional del Perú no necesita autorización del fiscal ni orden judicial para la incautación de los objetos, instrumentos, efectos o ganancias del delito o cualquier otro bien proveniente del delito o al servicio de la organización criminal, cuando se trate de una intervención en flagrante delito o peligro inminente de su perpetración, debiendo darse cuenta inmediata de su ejecución al fiscal.

Artículo 18. Proceso de pérdida de dominio Son de aplicación las reglas y el procedimiento del proceso de pérdida de dominio para los bienes señalados en el anterior artículo, siempre que se presente uno o más de los supuestos previstos en el artículo 4 del Decreto Legislativo 1104, que modifica la legislación sobre pérdida de dominio.

Perú

Artículo 23. Consecuencias accesorias cuando sean cometidos en ejercicio de la actividad de una persona jurídica o valiéndose de su estructura organizativa para favorecerlo, facilitarlo o encubrirlo, para la aplicación de las medidas previstas en el inciso 1 del presente artículo, el Juez tiene en consideración los criterios establecidos en el artículo 105-A del Código Penal.

Asimismo, el Código Penal peruano establece en sus artículos 221 y 224 las figuras de la Incautación preventiva y comiso definitivo de los aparatos, materiales o medios utilizados para la comisión del delito, de los activos y de cualquier evidencia documental etc. relacionada con el delito, lo solicita el Fiscal al Juez quien autoriza la incautación, así como autoriza el allanamiento y descerraje del local donde estuviere cometiéndose el delito.

El Código Procesal Penal no establece medidas de investigación tecnológica, en la investigación de este tipo de delitos 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

.

¿Quién las puede solicitar y quién acordar o autorizar?

Las puede solicitar el Ministerio Público. En Honduras se ha nombrado un juez de garantías que conoce exclusivamente de las solicitudes para la intervención telefónica

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

No pueden es una competencia exclusiva del Ministerio Público, y solo pueden autorizarse mediante autorización de un juez de garantías en la investigación, persecución, y el procesamiento de los delitos en que se requiera la utilización de esta técnica especial, valorando para ello la gravedad, utilidad y proporcionalidad de la medida en relación al delito que se trate.

Perú

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

La ley se rige por los principios de proporcionalidad, necesidad, idoneidad, confidencialidad, reserva jurisdiccional, temporalidad

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

No, todas necesitan de autorización judicial porque son esencialmente restrictivas de derechos fundamentales,

FORO GENERAL - MODULO 3 - TECNICAS DE INVESTIGACION EN PERU
de María del Carmen Victoria Ruiz - domingo, 29 de noviembre de 2020, 09:52
Número de respuestas:

3 Imagen de PERÚ

1.- Cuáles son las concretas medidas tecnológicas de investigación criminal que contempla su sistema legal, su Código Procesal Penal?

El Código Procesal Peruano aprobado por Decreto Legislativo 957 del 29.07.2004, 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. Entre las medidas principales tenemos:

1.1.- La Videovigilancia ordenada por el Fiscal de oficio o a pedido de la Policía, se requiere de autorización judicial cuando es realizada en lugares cerrados o al interior de un inmueble.

1.2.- El allanamiento y registro domiciliario, la incautación con registro y detención de personas, la exhibición forzada e incautación en sus Artículos 214, 217 y 218, Control de comunicaciones y documentos privados – 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. Artículo 231.- Registro de la intervención de comunicaciones telefónicas o de otras formas de comunicación, Artículo 232.- Aseguramiento e incautación de documento privado que no tenía orden de incautación, Art. 235.-

El levantamiento del secreto bancario, reserva tributaria, Artículo 237.- Clausura o vigilancia de locales e inmovilización.

Perú

1.3.- Asimismo se ha regulado las medidas de coerción procesal de restricción de derechos fundamental con expresa autorización judicial y con respeto al principio de proporcionalidad, necesidad, idoneidad, racionalidad, y que existan suficientes elementos de convicción, tales como la detención preliminar, la prisión preventiva, así como prevé la suspensión preventiva de derechos y otras medidas reales como medidas anticipativas (art. 312), medidas preventivas y cautelares contra personas jurídicas, y la Incautación.

1.4.- Los actos especiales de investigación como: Art. 340.- Circulación y entrega vigilada de bienes delictivos, Art. 341.- Agente encubierto y agente especial y Art. 341-A.- Operaciones encubiertas.

1.5.- También se ha regulado en la Ley 30077 Medidas coercitivas y técnicas especiales de Investigación en el marco de la Ley de Crimen Organizado, que comprende:

Artículo 8. Interceptación postal e intervención de las comunicaciones. En el ámbito de la presente Ley, se respetan los plazos de duración de las técnicas especiales de interceptación postal e intervención de las comunicaciones previstas en el inciso 2 del artículo 226 y en el inciso 6 del artículo 230 del Código Procesal Penal aprobado por Decreto Legislativo 957, respectivamente. 2. El trámite y realización de estas medidas tienen carácter reservado e inmediato.

Artículo 9. Interceptación postal 1. Solo se intercepta, retiene e incauta la correspondencia vinculada al delito objeto de investigación vinculado a la organización criminal, procurando, en la medida de lo posible, no afectar la correspondencia de terceros no involucrados.

Artículo 10. Intervención de las comunicaciones, Artículo 13. Agente encubierto, Artículo 14. Acciones de seguimiento y vigilancia.

Artículo 15. Deber de colaboración y de confi dencialidad de las instituciones y entidades públicas y privadas 1. Todas las instituciones y organismos del Estado, funcionarios y servidores públicos, así como las personas naturales o jurídicas del sector privado están obligadas a prestar su colaboración cuando les sea requerida para el esclarecimiento de los delitos regulados por la presente Ley, a fi n de lograr la eficaz y oportuna realización de las técnicas de investigación previstas en este capítulo.

2. La información obtenida como consecuencia de las técnicas previstas en el presente capítulo debe ser utilizada exclusivamente en la investigación correspondiente, debiéndose guardar la

Perú

más estricta confidencialidad respecto de terceros durante y después del proceso penal, salvo en los casos de presunción de otros

Incautación y Decomiso

Atículo 17. Procedencia En todas las investigaciones y procesos penales por delitos cometidos a través de una organización criminal, según lo previsto por la presente Ley, la Policía Nacional del Perú no necesita autorización del fiscal ni orden judicial para la incautación de los objetos, instrumentos, efectos o ganancias del delito o cualquier otro bien proveniente del delito o al servicio de la organización criminal, cuando se trate de una intervención en flagrante delito o peligro inminente de su perpetración, debiendo darse cuenta inmediata de su ejecución al fiscal.

Artículo 18. Proceso de pérdida de dominio Son de aplicación las reglas y el procedimiento del proceso de pérdida de dominio para los bienes señalados en el anterior artículo, siempre que se presente uno o más de los supuestos previstos en el artículo 4 del Decreto Legislativo 1104, que modifica la legislación sobre pérdida de dominio.

Artículo 23. Consecuencias accesorias cuando sean cometidos en ejercicio de la actividad de una persona jurídica o valiéndose de su estructura organizativa para favorecerlo, facilitarlo o encubrirlo, para la aplicación de las medidas previstas en el inciso 1 del presente artículo, el Juez tiene en consideración los criterios establecidos en el artículo 105-A del Código Penal.

Asimismo, el Código Penal peruano establece en sus artículos 221 y 224 las figuras de la Incautación preventiva y comiso definitivo de los aparatos, materiales o medios utilizados para la comisión del delito, de los activos y de cualquier evidencia documental etc. relacionada con el delito, lo solicita el Fiscal al Juez quien autoriza la incautación, así como autoriza el allanamiento y descerraje del local donde estuviere cometiéndose el delito.

Perú

Normatividad que en su país regula la investigación tecnológica restrictiva de Derechos Fundamentales

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 acusario 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. Artículo 231.- Registro de la intervención de comunicaciones telefónicas o de otras formas de comunicación, Artículo 232.- Aseguramiento e incautación de documento privado que no tenía orden de incautación, Art. 235.- El levantamiento del secreto bancario, reserva tributaria, Artículo 237.- Clausura o vigilancia de locales e inmovilización, asimismo medidas anticipativas (art. 312), medidas preventivas y cautelares contra personas jurídicas, y la Incautación. Los actos especiales de investigación como: Art. 340.- Circulación y entrega vigilada de bienes delictivos, Art. 341.- Agente encubierto y agente especial y Art. 341-A.- Operaciones encubiertas.

Así como se ha regulado mediante Ley especial 30077 Medidas coercitivas y técnicas especiales de Investigación en el marco de la lucha contra el Crimen Organizado que viene avanzando en nuevas manifestaciones de crimen tecnológico y sofisticado que teje redes ilícitas y criminaliza el Estado por su penetración en los aparatos de poder y en política, siendo que el Estado peruano ha dado esta Ley que complementa las medidas tecnológicas del Código Procesal Penal, y comprende: Técnicas Especiales de

Perú

Interceptación postal e intervención de las comunicaciones que tienen plazos de duración cuyo trámite y realización de estas medidas tienen carácter reservado e inmediato.

Se ha establecido que todas las instituciones y organismos del Estado, funcionarios y servidores públicos, así como las personas naturales o jurídicas del sector privado están obligadas a prestar su colaboración cuando les sea requerida para el esclarecimiento de los delitos regulados por Ley, a fin de lograr la eficaz y oportuna realización de las técnicas de investigación previstas, así como que la información obtenida debe ser utilizada exclusivamente en la investigación correspondiente, debiéndose guardar la más estricta confidencialidad respecto de terceros durante y después del proceso penal, salvo en los casos de presunción de otros delitos señalando el procedimiento a seguir.

¿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.

República Dominicana

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

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 los ciberdelitos económicos que contempla su legislación?

No informa

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

No informa

Normatividad que en su país regula la investigación tecnológica restrictiva de Derechos Fundamentales

No informa

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

Sistema legal, su Código Procesal Penal? Nuestro Código Penal no contempla ninguna medida tecnológica de investigación criminal para perseguir los crímenes y delitos cibernéticos, pero en al 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)

¿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

¿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.

Uruguay

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

En Uruguay el Código Penal que ha tenido modificaciones recientemente a través de una ley de Urgente consideración que impulso el nuevo gobierno, no se han realizado inclusión alguna de los ciberdelitos.

Esto se debe a que si bien el país ha ratificado el convenio en Madrid en el año 2014, por razones de funcionamiento del Poder Legislativo, no se ha transformado en ley debido a que se archivabó al finalizar el periodo legislativo y recién con fecha 9 de octubre 2020 por informe del Ministerio del Uruguayo se elevó a la Asamblea General.

¿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 los ciberdelitos económicos que contempla su legislación?

No informa

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

En Uruguay se contempla como medios tecnológico la interceptación de llamadas telefónicas whatsaap 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.

¿Quiénes pueden solicitar y decretar estas medidas?

La solicita el titular de la Acción Penal y la dectreta el Juez

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

Actualmente en el país esta vigente el articulo 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 a 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.

¿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?

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.

Uruguay

Normatividad que en su país regula la investigación tecnológica restrictiva de Derechos Fundamentales

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.

SISTEMATIZACIÓN DEL CURSO VIRTUAL

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

Del 23 de noviembre al 4 de diciembre de 2020
Cartagena de Indias

Consejo General del Poder Judicial

Aula Iberoamericana
Consejo General del Poder Judicial

Cooperación Española
CONOCIMIENTO / INTERCOONECTA