

CONCLUSIONES Y

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

Costa Rica dentro de su legislación no tipifica los ciberdelitos dentro de un título o capítulo; sin embargo, el código penal costarricense cuenta con tipos penales relacionados con ~~este tipo de~~ delincuencias.

Los ciberdelitos fueron introducidos en la legislación costarricense en el año 2001, mediante reforma al ~~código p~~Penal, ~~por medio del cual~~ se promulgaron los tipos penales de violación de comunicaciones electrónicas, fraude electrónico y alteración de datos y sabotaje informático, numerales 196 ~~bis~~, 2017 ~~bis~~ y 229 ~~bis~~, respectivamente.

~~Posteriormente~~ En el año 2012, mediante reforma legislativa al ~~código p~~Penal denominada "*Reforma de Varios Artículos y Modificación de la Sección VIII, Denominada Delitos Informáticos y Conexos, del Título VII del Código Penal*", entraron en vigencia los siguientes tipos penales:

- Artículo 167.- Corrupción.
- Artículo 196.- Violación de correspondencia o comunicaciones.
- Artículo 196 *bis*. - Violación de datos personales.
- Artículo 214.- Extorsión.
- Artículo 217 *bis*. - Estafa informática. (derogando el fraude informático)
- Artículo 229 *bis*. - Daño informático.
- Artículo 229.- Daño agravado.
- Artículo 229 ~~ter.~~ - Sabotaje informático.
- Artículo 230.- Suplantación de identidad.
- Artículo 231.- Espionaje informático.
- Artículo 232.- Instalación o propagación de programas informáticos maliciosos.
- Artículo 233.- Suplantación de páginas electrónicas.
- Artículo 234.- Facilitación del delito informático.
- Artículo 235.- Narcotráfico y crimen organizado.
- Artículo 236.- Difusión de información falsa.

¿Cuáles son los ciberdelitos económicos que contempla su legislación?

La legislación penal de Costa Rica contempla las siguientes figuras típicas relacionadas con ciberdelincuencia económica:

- Estafa Informática.
- Sabotaje Informático.
- Espionaje Informático.
- Instalación o Propagación de Programas Informático Maliciosos.

Con formato: Fuente: Cursiva

Con formato: Fuente: Cursiva

Con formato: Fuente: Cursiva

Con formato: Fuente: Cursiva

Con formato: Fuente: Cursiva

Por otra parte, mediante ley número 9877, “*Ley Contra el Acoso Sexual Callejero*” de fecha 27 de agosto del 2020, se incorporó al código penal el numeral 175 *quinquies* el delito de Producción de Material Audiovisual.

Con formato: Fuente: Cursiva

Con formato: Fuente: Cursiva

Finalmente, mediante ley número 10020 “*Ley para la prevención del acoso a personas menores de edad por medios electrónicos o virtuales (GROOMING)* y reforma Código Penal”, de fecha 10 de abril del 2021, modificó y amplió los siguientes artículos:

Con formato: Fuente: Cursiva, Color de fuente: Negro

Con formato: Fuente: Cursiva, Color de fuente: Negro, Diseño: Claro (Blanco)

- Artículo 167.- Corrupción.
- Artículo 167 *bis*- Seducción o encuentros con persona menor de edad o incapaz por medios electrónicos.
- Artículo 168- Corrupción agravada.
- Artículo 173- Fabricación, producción, o reproducción de pornografía.
- Artículo 173 *bis*- Tenencia de material pornográfico.
- Artículo 174- Difusión de pornografía.

¿Cuáles son los ciberdelitos intrusivos que contempla su legislación?

La legislación penal de Costa Rica contempla los siguientes ciberdelitos intrusivos:

- Corrupción.
- Violación de correspondencia o comunicaciones.
- Violación de datos personales.
- Estafa informática.
- Daño informático.
- Daño agravado.
- Sabotaje informático.
- Suplantación de identidad.
- Espionaje informático.

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

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

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

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

Actualmente en Costa Rica la normativa procesal penal no contempla formalmente en código de rito, procedimiento alguno de investigación que regulen investigaciones mediante medidas tecnológicas, no obstante, en virtud de que nos rigen principios tales como los de objetividad, legalidad y libertad probatoria, descritos regulada en los artículos 180, 181 y 182 del código procesal penal, es viable hacer uso de cualquier medio probatorio mientras este sea legal. Por otra parte, en donde podría indicarse que la regulación que existe regulación escueta y que se utiliza para la recopilación de este tipo de elementos probatorios tecnológicos, es la Ley Sobre el Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones o Ley Número 7425 del 09 de agosto de 1994.

¿Quiénes pueden solicitar y decretar estas medidas?

Las relacionadas a la Ley Sobre el Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones y de acuerdo al artículo 24 de la Constitución Política de Costa Rica, para, son solicitadas por el Ministerio Público quien por imperativo legal tiene a cargo la investigación, gestión que debe de ser planteada ante el juez penal de la etapa correspondiente, por ende, corresponde a la autoridad jurisdiccional decretar la medida.

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

Es factible que las partes, o bien los investigadores, aporten elementos de prueba tecnológica tales como videos, fotografías, enlaces, capturas, grabaciones de audio, etc), siempre y cuando no se esté bajo los supuestos establecidos en la Ley Sobre el Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones; es decir, que no violentan alguno de los derechos fundamentales y hayan sido recopiladas mediante medios lícitos.

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

En Costa Rica si bien no existe normativa específica que regule medidas de investigación tecnológica, se cuenta con un control de garantías realizado por la persona juzgadora ~~el juez~~ a partir de normas generales del Código Procesal Penal y de la Ley Sobre el Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones.

Esta ~~normativa~~ exige al tribunal que para otorgar autorizaciones deben cumplirse los principios y garantías de la constitución, derecho internacional y comunitario y prohíbe al Ministerio Público realizar dichos actos sin la autorización o supervisión de la ~~autoridad jurisdiccional~~ ~~el juez~~.

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

El ordenamiento jurídico costarricense y la puesta en práctica de dichas normas en su realidad jurídica es garantista, de tal forma la actuación de la persona juzgadora al analizar la posibilidad de aplicación de una medida tecnológica para recopilación de prueba o bien para la admisión de dicha prueba (así como de cualquier otra), se regulan en el artículo 183 y siguientes del Código Procesal Penal, siempre regirá la legalidad, pero además se tomarán en cuenta principios de especialidad, idoneidad, necesidad y excepcionalidad y proporcionalidad.

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

Sí, la normativa existente en Costa Rica que faculta a utilizar un micrófono como medida de investigación, se encuentra establecido en los artículos 9 al 13 de la Ley Sobre el Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones.

Autorización de intervenciones: Dentro de los procedimientos de una investigación policial o jurisdiccional, los tribunales de justicia podrán autorizar la intervención de comunicaciones orales, escritas o de otro tipo, incluso las telecomunicaciones fijas, móviles, inalámbricas y digitales, cuando involucre el esclarecimiento de los siguientes delitos: secuestro extorsivo, corrupción agravada, proxenetismo agravado, fabricación, producción o difusión de pornografía y delitos sexuales contra personas menores de edad; trata de personas, tráfico ilícito de migrantes y tráfico de órganos; homicidio calificado, femicidio, genocidio, terrorismo y los delitos previstos en la Ley 7786, Ley sobre Estupefacientes, Sustancias Psicotrópicas, Drogas de Uso No Autorizado, Actividades Conexas, Legitimación de Capitales y Financiamiento al Terrorismo, de 30 de abril de 1998, así como los delitos de corrupción contra los deberes de la función pública que se indican: cohecho impropio, cohecho propio, corrupción agravada, aceptación de dádiva por acto cumplido, corrupción de jueces, penalidad del corruptor, concusión, prevaricato, peculado, malversación, peculado y malversación de fondos privados, enriquecimiento ilícito, legislación o administración en provecho propio, sobreprecio irregular, tráfico de influencias, soborno transnacional, influencia en contra de la Hacienda Pública, fraude de ley en la función administrativa.(...)

Orden del Juez para intervenir: El Juez, mediante resolución fundada, de oficio, a solicitud del Jefe del Ministerio Público, del Director del Organismo de Investigación Judicial o de alguna de las partes del proceso, si hubiere, podrá ordenar intervenir las comunicaciones orales o escritas, cuando pueda servir como prueba indispensable de la comisión de alguna de las conductas delictivas, a las que se refiere el artículo anterior.

El Juez realizará personalmente la diligencia, salvo en casos de excepción en los cuales, según su criterio, podrá delegarla en miembros del Organismo de Investigación Judicial o del Ministerio Público, quienes deberán informarle, por escrito, del resultado. De ello deberá levantarse el acta correspondiente.

La solicitud de intervención deberá estar por escrito, expresar y justificar sus motivos y cometidos, con el propósito de que puedan ser valorados por el Tribunal. En caso de que sea solicitada por el Organismo de Investigación Judicial deberá contener, además, los nombres de los oficiales a cargo de la investigación. En los demás casos, el Juez solicitará a ese Organismo la designación respectiva.

Contenido de la autorización para intervenir: La resolución mediante la cual se autorice intervenir las comunicaciones orales o escritas, deberá contener, so pena de nulidad:

- La indicación expresa del hecho que se pretende esclarecer.
- El nombre del dueño o del usuario del medio de comunicación por intervenir o del destinatario de la comunicación y su vínculo con los hechos.
- El período durante el cual tendrá vigencia la medida ordenada.
- El nombre de la oficina y de los funcionarios autorizados para realizar la intervención.

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

En Costa Rica, priva un principio de libertad probatoria relacionado con el principio de legalidad, lo que significa que es permitido realizar todo tipo de diligencias de investigación siempre y cuando la captación no constituya como prohibida, siendo que es permitido realizar medidas tecnológicas de investigación sin autorización judicial siempre que no afecten derechos fundamentales y dentro de las que existen las siguientes:

- Estudio de geolocalización por radio bases.
- Análisis de registros telefónicos.
- Análisis de datos de tráfico
- Análisis de datos de suscriptor abonado.
- Técnica de investigación en fuentes abiertas
- Solicitudes de preservas de datos a proveedores de servicios o instituciones.
- Secuestros de cámaras de video y fotografías
- Secuestro de dispositivos electrónicos.

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

En cuanto a la colocación de dispositivos de ubicación o mediante GPS, no existe regulación alguna; sin embargo, la Sala Constitucional en un fallo determinó que la colocación de dicho instrumento debe ser ordenada por autoridad jurisdiccional. Al respecto señaló: "El recurrente argumentó que existe únicamente un límite al derecho de acceso a la información administrativa, el secreto de estado. Sin embargo, según se expuso en la sentencia citada, existen también límites extrínsecos, reiteradamente reconocidos por esta Sala y por la doctrina. Entre ellos está el derecho de todas las personas a una esfera de intimidad, garantizado en el artículo 24 de la Constitución Política. En el caso concreto, los datos obtenidos con el sistema GPS podrían revelar la localización exacta de lugares que, en su ámbito privado, frecuenta el funcionario e, incluso, la de las casas de habitación

Con formato: Justificado

Con formato: Fuente: Cursiva

Con formato: Fuente: Negrita, Cursiva

de otras personas, como familiares o allegados, a los que es razonable suponer que visita. A juicio de esta Sala, tal información sí está protegida por el artículo 24 constitucional. De igual manera, la información podría revelar, de manera exacta, hábitos de desplazamiento, lo que pone en riesgo la seguridad de funcionarios que ocupan altos cargos. Es razonable que exista un régimen especial, que impide separar de manera clara el uso del vehículo para asuntos estrictamente oficiales y aquellos que obedecen a razones particulares del titular del puesto. La calificación del vehículo como de uso discrecional no es antojadiza; se trata de una disposición legislativa -como bien señaló el Jefe de Departamento de Transportes- que obedece, entre otras, a la razón antes expuesta" (Sala Constitucional, v. 2011-12389, de las 13:10 hrs. del 9 de setiembre de 2011). [...] (La negrita de suple)

Con formato: Fuente: Cursiva

Con respecto a otras herramientas de geolocalización, se pueden utilizar atendiendo al principio de libertad a probatoria, siempre que no afecten garantías fundamentales, caso en el que se requiere autorización judicial.

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

Respecto a este tema en Costa Rica, deben de diferenciarse diferentes estadios, el primero de ellos que es la custodia de la evidencia, ello ha sido ampliamente discutido, existe basta jurisprudencias, así mismo los funcionarios reciben ~~en~~ ^{en} amplias capacitaciones respecto al adecuado manejo de cadena de custodia, aunado a ello la Defensa ~~Técnica Pública (quienes en su mayoría atienden los asuntos penales)~~ son sumamente celosos y contralores de ese adecuado manejo, ~~de tal suerte creo que modestia aparte dicho tema ya se encuentra debidamente superado en el país, Ahora bien en cuanto a la obtención de la evidencia digital, -actualmente junto a otro compañero, me encuentro desarrollando un ensayo al respecto, y es~~ que existe una falta de familiaridad o temor hacia lo novedoso, hacia lo tecnológico, ~~esto sumado a la falta de regulación procesal genera el lo cual sumado a lo garantista del proceso penal costarricense, se hacen~~ uso de prácticas no regladas, que buscan ~~aún más~~ proteger ese velo de una sana y adecuada obtención de la prueba, ~~lo cual torna en odioso y complicado en relación a los plazos, el tema del acceso y obtención de dicho tipo de prueba digital.~~



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

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

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

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

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

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

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

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

Los delitos mencionados, ¿son perseguibles de oficio o requieren la denuncia por parte de la víctima?

Son delitos de acción pública y por ende perseguibles de oficio

¿Han tenido lugar modificaciones legislativas en los últimos años para luchar contra la ciberdelincuencia de género?

En Costa Rica no se ha generado la iniciativa para integrar propiamente delitos de ciberdelincuencia enfocados en violencia de género

¿Establece su legislación medidas concretas de protección para las víctimas de ciberdelincuencia de género?

En Costa Rica si existen medidas de protección para víctimas de violencia de género en general, pero su regulación no es específica en materia de ciberdelincuencia de género.

¿Considera adecuada la legislación de su país sobre obligación de las operadoras de comunicación para la denuncia de delitos?

En la realidad nacional, las regulaciones para que las operadoras de comunicación proporcionen información para las investigaciones penales nacen de índole administrativo, mas no judiciales o a través de una forma llamada Sistema Informático de Solicitudes por parte de las empresas de telecomunicaciones que operan bajo las directrices del Ministerio Público y de la Policía Judicial, por dicho medio, sin control jurisdiccional, no se obtiene información para el caso de parte de las operadoras privadas, así mismo los plazos de

que se encuadra en el concepto de

La ley número 8589 denominada Ley de penalización de la violencia contra la mujer, la ley no contempla de manera específica un delito de violencia de género, pero si existen tipos penales que su alcance permite si son de violencia de género (amenazas, mensajes de texto, mensajes vía WhatsApp, redes sociales), aunque estrictamente el artículo no lo establece, dichos artículos son:

Artículo 177, Ley de penalización de la violencia contra la mujer, establece una medida de protección para las víctimas de violencia de género.

Artículo 177, “Ley Contra el Acoso Sexual Callejero” de fecha 2017, establece en el código penal el numeral 175 quinquies el delito de

Produccion de Material Audiovisual.

