PERFIL CRIMINOLÓGICO

FISCALÍA GENERAL DEL ESTADO

FGE

FISCALÍA GENERAL DEL ESTADO

ECUADOR

Edición

PERFIL CRIMINOLÓGICO 30

Revista Científica de Ciencias Jurídicas, Criminología y Seguridad
FISCALÍA GENERAL DEL ESTADO

Quito, diciembre de 2021

PERFIL CRIMINOLÓGICO

Presentación

Siguiendo la tradición de abordar temas de enorme importancia para el mundo del derecho penal, la Revista Científica de Ciencias Jurídicas, Criminología y Seguridad, Perfil Criminológico, se adentra en el análisis de las nuevas modalidades del delito, específicamente, el cibercrimen en su contexto integral.

¿Por qué es importante el tratamiento de esta temática? La respuesta la podemos encontrar al regresar la mirada al avance de la tecnología y la globalización, que a la vez que han servido para facilitar las actividades del ser humano en todas las áreas del conocimiento, ha sido aprovechado por los ciudadanos que actúan al margen de la ley, que utilizando esas herramientas, quebrantan la voluntad de las personas; así como de seguridades, mecanismos y procedimientos para atentar en contra de bienes jurídicos protegidos, llegando a consolidarse desde ya, en la empresa delictual con mayor futuro en el presente siglo.

No existe área de las actividades del ser humano que quede exenta de los tentáculos del cibercrimen. Así, el patrimonio, la salud pública, la integridad sexual y reproductiva, están entre los bienes jurídicos más vulnerados a través de esta modalidad ilícita, por lo general con característica de transnacionalidad, afectando simultáneamente a varios países. De ahí la importancia de su abordaje en la presente publicación.

En esta edición, contamos con el aporte de connotados profesionales del derecho, quienes con su basto conocimiento del tema y a la vez, la facilidad de trasmisión de conocimientos, generaron un elemento editorial que se constituye en una fuente de reflexiones necesarias para el estudiante, el profesional del derecho y el ciudadano en general, en la amplitud del horizonte que se abre, para entender en su real dimensión, la cibercriminalidad.

Entre los temas planteados encontraremos: El rol de la Justicia y la Cooperación Internacional en la lucha contra la ciberdelincuencia, abordado por la Dra. Diana Salazar Méndez, Fiscal General del Estado, quien con su preparación académica y experiencia, nos describe como la Fiscalía hace frente a la investigación y procesamiento de esta clase de delitos, considerando la especialización; así como los diferentes mecanismos de cooperación internacional para la eficacia en el acopio de elementos probatorios existente en otros países.

Conoceremos sobre la estrategia de nuestro país sobre ciberseguridad, tema tratado por el señor Ing. Gabriel Llumiquinga Veintimilla, distinguido catedrático de nuestro país, que nos pone en el contexto de modelos internacionales en Ciberseguridad, entre ellos de Singapur; y, las recomendaciones para el reajuste del modelo óptimo para Ecuador.

La omisión impropia en los delitos de apropiación fraudulenta por medios electrónicos, transferencia electrónica de un activo patrimonial y la responsabilidad penal de los administradores de las instituciones del sistema financiero, es tratado por el distinguido Catedrático y Ex-Juez de Corte Provincial, Dr. Santiago Acurio Del Pino. Se analiza desde la dogmática y jurisprudencia como "la no evitación del resultado equivale a su producción", en los delitos de apropiación fraudulenta por medios electrónicos y transferencia electrónica de activo patrimonial, conocidos como delitos de omisión impropia, esto desde la función de garante que les otorga la Constitución, la Ley y el contrato, a los administradores de las instituciones del sistema financiero y los funcionarios subyacentes.

No menos importante resulta el estudio de las dificultades en la investigación y persecución de los cibercrímenes, tema tratado por el maestro Ricardo Posada Maya, catedrático universitario de la república de Colombia, resaltando el hecho que los operadores del sistema de justicia penal no siempre distinguen entre los delitos informáticos en sentido general y los cibercrímenes en particular, lo cual cataloga como una causa que afecta al sistema.

En definitiva, los temas y autores por sí solos, constituyen un aliciente para los interesados en el derecho penal. Así, no dejemos de leer el contenido de esta revista, en su integridad, para tener una concepción clara y amplia del cibercrimen y su incidencia en la afectación a la seguridad de la sociedad ecuatoriana y mundial.

Wilson Toainga Toainga
Fiscalía General del Estado Subrogante

PERFIL CRIMINOLÓGICO

EL ROL DE LA ADMINISTRACIÓN DE JUSTICIA Y LA COOPERACIÓN INTERNACIONAL EN LA LUCHA CONTRA LA CIBERDELINCUENCIA

DIANA SALAZAR MÉNDEZ[1]

Introducción

El ciberespacio, que configura un espacio comunicativo e interactivo paralelo al mundo físico, ha modificado significativamente las relaciones económicas, políticas, sociales y personales2[2]. Internet ha desafiado los fundamentos del comportamiento delictivo, permitiendo a los delincuentes que residen en una jurisdicción cometer delitos en otra, mientras blanquean dinero en una tercera.

El ciberdelito es una forma desarrollada de crimen transnacional. La naturaleza compleja del delito cibernético es su participación en grupos delictivos organizados. Junto a esto, los delincuentes y las víctimas se encuentran en diferentes regiones, y sus efectos pueden extenderse a sociedades de todo el mundo, requiriendo una respuesta urgente, dinámica e integrada3[3].

Múltiples capas de cifrado de identidad garantizan a los delincuentes un anonimato casi completo, y las monedas virtuales permiten de manera similar transacciones sin rastro. Usando estas tecnologías, los grupos delictivos perpetúan una variedad de actos criminales que van desde la explotación sexual de niños en línea, el robo de identidad y los fraudes, hasta la configuración de áreas digitales seguras donde se pueda realizar el intercambio de servicios criminales4[4].

---

1 Fiscal General del Estado (Ecuador).

2 Mario Ron, Walter Fuertes, Marco Bonilla, Theofilos Toulkeridis y Javier Díaz, "Cybercrime in Ecuador, an Exploration, which allows to define National Cybersecurity Policies", 2018 13th Iberian Conference on Information Systems and Technologies (CISTI), (2018):1-7.

3 Olena Sviatun, Olga Goncharuk, Chernysh Roman, Olena Kuzmenko y Ihor Kozych, "Combating cybercrime: economic and legal aspects", WSEAS Transactions on Business and Economics 18, n.° 1 (2021):751-762.

4 Tuesday Reitano, Troels Oerting y Marcena Hunter, "Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce (J-CAT)", The European Review of Organised Crime 2, n.° 2 (2015): 142-154.

Las instituciones supranacionales también se han visto perturbadas por los ciberdelitos políticos o ideológicos, la ciberguerra, el hacktivismo y el ciberterrorismo. Tales conductas se han utilizado para desestabilizar un Estado o para difundir mensajes políticos aprovechando la comunicación masiva que ofrece el ciberespacio. Los ataques de denegación de servicio, infecciones de malware u otras acciones similares continúan paralizando la actividad de importantes instituciones de un país, provocando múltiples daños, incluida la pérdida de beneficios.

En efecto, el ciberdelito ha demostrado que es una de las mayores amenazas para la economía mundial. Para las empresas, los costes y las pérdidas relacionadas con el ciberdelito son enormes: combinan corrupción y destrucción de datos, robo de fondos, propiedad intelectual, datos personales y financieros, interrupción del negocio después de un ciberataque, daño a la reputación empresarial, pérdida de productividad, etc. Los datos disponibles respaldan estas preocupaciones[5]. Según un reciente informe del Banco Interamericano de Desarrollo, se estima que los daños por delitos cibernéticos alcanzarán los seis billones de dólares para el año 2021, lo que equivale al producto interno bruto (PIB) de la tercera economía más grande del mundo[6].

Lucha contra la ciberdelincuencia: panorama institucional

La seguridad es un bien público que puede verse amenazado por la delincuencia. Hoy en día, no solo la seguridad en el mundo offline, sino también la seguridad en el ciberespacio es un valor que debe garantizarse[7]. En consecuencia, consciente de la importancia de la implementación de una normativa que permita una adecuada lucha contra la criminalidad informática, el Estado ecuatoriano en su Constitución Política, como norma jurídica fundamental, considera la responsabilidad de desarrollar políticas que protejan los derechos de las personas, en este caso, para brindar protección al uso del ciberespacio. En este orden de ideas, en el país, los ciberdelitos están tipificados en el Código Orgánico Integral Penal (COIP) como una medida para perseguirlos y fijar sanciones.

Desde la entrada en vigencia del COIP, en el año 2014, el Sistema Integrado de Actuaciones Fiscales (SIAF) de la Fiscalía General del Estado ha registrado un número significativamente creciente de denuncias en este ámbito de criminalidad. En particular, el número de denuncias se concentra, entre otros, en delitos como el contacto con finalidad sexual con menores de dieciocho años por medios electrónicos *(child grooming)*: 829 denuncias desde 2014; apropiación fraudulenta por medios electrónicos: 10.393 denuncias desde 2014; transferencia electrónica de activo patrimonial: 387 denuncias desde 2014; acceso no consentido a un sistema informático, telemático o de telecomunicaciones: 829 denuncias desde 2014.

Para combatir el ciberdelito en forma real, es necesario reconocer e identificar su origen, sus causas, motivaciones y múltiples actores[8]. Todo ello transcribe políticas nacionales, empresariales y personales, así como la creación de métodos y herramientas tecnológicas que permitan al usuario ejercer pragmáticamente el derecho a protegerse. En este escenario, además, la idoneidad del derecho penal es de gran importancia para el enjuiciamiento del delito cibernético, ya sea nacional o internacional.

Sin embargo, con frecuencia, las innovaciones criminales asociadas al delito cibernético han revelado las limitaciones de las instituciones diseñadas para la seguridad nacional y la aplicación de la ley[9]. En efecto, el ciberdelito es una amenaza inmensa que plantea varios desafíos para el derecho penal tradicional y el sistema de justicia en general[10].

5 Sviatun et al., "Combating cybercrime: economic and legal aspects".

6 Banco Interamericano de Desarrollo, Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe (Washington: Banco Interamericano de Desarrollo, 2020), https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

7 Reitano, Oerting y Hunter, "Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce (J-CAT)".

8 George Christou, "The challenges of cybercrime governance in the European Union", European Politics and Society 19, n.° 3 (2018): 355-375.

9 Reitano, Oerting y Hunter, "Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce (J-CAT)".

10 Francesco Calderoni, "The European legal framework on cybercrime: striving for an effective implementation", Crime, Law and Social Change 54, n.° 5 (2010): 339-357.

El primer desafío es que las tecnologías de la información y la comunicación (TIC) son complejas y, con frecuencia, desconocidas para el mundo de la justicia penal tradicional. Así, la creación de leyes y normas de buenas prácticas ha sido más lenta que la evolución del desarrollo del ciberdelito y la formación de los operadores de justicia sigue siendo un desafío[11].

Tratar los delitos que involucran estos dispositivos requiere de personal bien capacitado en la fase de investigación, durante el enjuiciamiento y en los tribunales. De este modo, si los conocimientos tecnológicos e informáticos resultan relativamente ajenos a la aplicación de la ley y las culturas legales, los Estados deben invertir en capacitación y educación constante[12].

Como segundo desafío, muchos delitos cibernéticos ocurren con frecuencia en diferentes lugares, que pueden estar bajo la jurisdicción de distintos países. En este sentido, uno de los obstáculos más importantes en la investigación es determinar dónde se originó el delito. Esto no siempre es evidente a partir de la dirección y la información de enrutamiento[13]. Un ataque que parece haber sido lanzado desde un país cercano bien puede haberse originado en otro lugar y haber pasado por numerosas jurisdicciones antes de su última dirección.

Así, cuando la actividad delictiva se origina en un país, transita por uno o más países intermedios y genera pérdidas o daños en el país de destino, ¿dónde ha ocurrido el delito? Esta naturaleza virtual de los delitos cibernéticos requiere que los países establezcan reglas claras sobre la jurisdicción de un sistema legal sobre estos delitos. Al respecto, los Estados soberanos son libres de definir cualquier comportamiento como criminal, sujeto a los poderes que les otorguen o las restricciones impuestas por sus correspondientes constituciones[14].

El tercer desafío es que el mundo de las TIC se mueve a un ritmo diferente al del mundo físico. Los delitos ocurren en una fracción de segundo y pueden propagarse a una velocidad asombrosa. Además, la evidencia de un delito cibernético suele consistir en información digital, que es efímera y volátil por naturaleza y puede modificarse o eliminarse[15].

Por tanto, los organismos encargados de hacer cumplir la ley deben tomar medidas rápidas y ser capaces de recopilar y preservar pruebas digitales para su uso en procesos penales. Aquellos casos que requieren investigación en tiempo real no permiten una investigación pausada. Incluso el acceso a la información almacenada puede requerir una acción oportuna. Los proveedores de servicios de Internet no almacenan datos de transacciones para siempre y los requisitos de retención, cuando existen, son limitados.

En este sentido, así como los gobiernos, en el espacio terrestre, no pueden permitirse el lujo de desplegar agentes de policía en cada esquina de las calles, los recursos para hacer cumplir la ley también son limitados en el mundo digital. De este modo, considerando la necesidad de generar estrategias alternativas para hacer frente a este tipo de criminología, las instituciones comerciales, desde la industria de la seguridad informática hasta la industria de los seguros y los especialistas del sector privado en informática forense, pueden desempeñar un papel importante en la prevención y el control del delito cibernético[16].

11 Ron et al., "Cybercrime in Ecuador, an Exploration, which allows to define National Cybersecurity Policies".

12 Calderoni, "The European legal framework on cybercrime: striving for an effective implementation

13 Ana Cerezo, Javier Lopez y Ahmed Patel. "International Cooperation to Fight Transnational Cybercrime", Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007), (2007): 13-27.

14 Marc Goodman, "International Dimensions of Cybercrime", en Cybercrimes: A Multidisciplinary Analysis, ed. Sumit Ghosh y Elliot Turrini (Berlín: Springer, 2010), 311-339.

15 Calderoni, "The European legal framework on cybercrime: striving for an effective implementation".

16 George Christou, "The challenges of cybercrime governance in the European Union".

Por otro lado, debido a los retos excepcionales que presentan los delitos cibernéticos, la Fiscalía General del Estado, en coordinación con otras unidades investigativas, ha desarrollado diferentes programas de capacitación. Determinados eventos de formación se han enfocado dentro de todo el espectro de aplicación e injerencia de los delitos cibernéticos y han sido auspiciados por organismos internacionales como el Departamento de Estado, el Servicio de Pesca y Vida Silvestre de Estados Unidos, la Oficina de las Naciones Unidas contra la Droga y el Delito; así como por instituciones nacionales como la Dirección Nacional de Ciberdelitos de la Policía Nacional. Estas capacitaciones se han constituido como un significativo aporte a la investigación de los delitos cibernéticos, basadas en un enfoque holístico acorde a aspectos como investigación, presentación de evidencia y evaluación y análisis.

No obstante, el alcance, la escala y la estructura del ciberdelito sobrepasan la capacidad de cualquier organismo regulador único. En consecuencia, para montar una respuesta eficaz a una industria de la ciberdelincuencia en crecimiento exponencial, es fundamental que los organismos encargados de hacer cumplir la ley de todo el mundo colaboren, compartan inteligencia y alineen prioridades. Sin una cooperación significativa entre las naciones y la adopción de nuevas estrategias, la aplicación de la ley se quedará atrás, combatiendo el crimen del siglo XXI con herramientas del siglo XIX[17].

En efecto, la naturaleza interconectada y en red del ciberespacio, junto con el surgimiento del ciberdelito y la promulgación de nuevas leyes, hacen imperativo lograr coherencia en las prohibiciones penales internacionales; la solución más simple consistiría en crear un código legal único que regule los delitos cibernéticos y que sea válido en todo el mundo, independientemente de las leyes de cada nación. Esta solución no es viable en la actualidad, dado que ningún país se inclina a ceder sus propias leyes a favor de las leyes internacionales sobre delitos informáticos[18].

La alternativa, entonces, sería crear un marco normativo común, que consista en un conjunto de principios que cada país pueda utilizar para analizar su legislación existente para delitos tradicionales y enmendarla para enfrentar los desafíos de los delitos cibernéticos[19]. En general, la investigación revela que los casos de delitos cibernéticos tienen mayores probabilidades de procesarse y sancionarse en sociedades que se han caracterizado por un mayor grado de cooperación e integración y que se adhieren a marcos legislativos internacionales comunes.

En este contexto, específicamente el Convenio sobre la Ciberdelincuencia de Budapest establece la cooperación entre los Estados para combatir la ciberdelincuencia y proteger los intereses legítimos en el campo de las tecnologías de la información. El Convenio de Budapest se centra en tres elementos básicos: el primero es la importancia de las medidas legislativas sustantivas; el segundo elemento es la importancia de una legislación procesal adecuada a la naturaleza del delito; y, el tercero es la importancia de la cooperación internacional y regional en el campo del ciberdelito[20].

Además, la Convención sobre Delitos Cibernéticos describe métodos para recolectar evidencia digital en el curso de una investigación criminal. Estos métodos también son aplicables a la investigación del delito en general, es decir, no están reservados únicamente a los ciberdelitos. Estos métodos cumplen condiciones de compatibilidad con los derechos fundamentales de las personas. Consecuentemente, al autorizar la aplicación legal de los métodos, los Estados mejoran el marco legal para la cooperación internacional en la investigación criminal de delitos transfronterizos.

Sin embargo, en la medida en que sea necesario, cada Estado Parte o, en su defecto, que busque serlo iniciará o mejorará un proceso de modernización de los mecanismos de cooperación internacional en derecho penal. Un primer paso apunta a desarrollar leyes nacionales de manera con un enfoque integral que alineados a la legislación internacional de combate a la delincuencia sistemática. Además, dado que la cooperación judicial debe desarrollarse en sus diversas etapas, incluida la ejecución de las sentencias, es necesario identificar la posición actual de la política ejecutiva establecida y revisar el rol de los órganos de administración de justicia asociada a la implementación de leyes especializadas y la calidad de las mismas.

De este modo, con el objetivo de contar con un soporte legal que permita hacer frente a los delitos cibernéticos, la Fiscalía General del Estado ecuatoriano ha desarrollado las acciones necesarias –dentro de un proceso interinstitucional– para impulsar la adhesión del Ecuador a dicho Convenio. En este contexto, se han realizado varias reuniones junto al Ministerio de Gobierno, bajo la coordinación de Cancillería, y con el apoyo de la cooperación no reembolsable del Consejo de Europa y expertos de la iniciativa GLACY+.

Los delitos cibernéticos han negado la simplicidad[21]. Por ello, es importante mencionar que, con el apoyo de expertos y con el aval de El PAcCTO, la Fiscalía del Ecuador se encuentra en el proceso de creación de una unidad especializada contra la ciberdelincuencia. Al respecto, se cuenta con un informe que resume la situación actual del país en materia de ciberdelincuencia y sugiere aspectos para la creación y funcionamiento de la referida unidad especializada. Dicho informe es, además, parte de los insumos para promover la adhesión de Ecuador al Convenio de Budapest.

Por otro lado, a través de funcionarios designados como puntos de contacto, la Fiscalía ecuatoriana forma parte de varias redes y grupos regionales conformados dentro de diferentes organismos y foros internacionales en los que participa de manera activa; entre ellos, están: el Comité Ad-Hoc sobre Ciberdelito de la Oficina de Naciones Unidas contra la Droga y el Delito; el Comité Especial de Expertos de composición abierta para elaborar la Convención Internacional sobre la lucha contra el uso de las tecnologías de la información y las comunicaciones con fines delictivos; el Grupo de Trabajo en Delito Cibernético de las Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas (REMJA); la Red de Ciberdelincuencia de la Asociación Iberoamericana de Ministerios Públicos (AIAMP); y, por supuesto, colabora con la Subcomisión de Ciberdelito de la Reunión Especializada de Ministerios Públicos del MERCOSUR (REMPM).

La respuesta de los Estados debe ser urgente, dinámica e integrada. Por ello, si bien un marco sólido de legislación penal contra el delito cibernético es un requisito absoluto para la acción eficaz contra los delincuentes cibernéticos, es igualmente importante la legislación procesal actualizada, misma que autorizará la emisión de órdenes para registrar y confiscar pruebas tangibles. Como se señaló antes, el tiempo es esencial en los delitos cibernéticos, dado que la evidencia es altamente perecedera y depende de registros informáticos de corta duración. Por ello, la Fiscalía General del Estado, en su afán de combatir la ciberdelincuencia, se ha alineado con los requerimientos internacionales en el uso de las tecnologías de la información para la transmisión y recepción inmediata de solicitudes de asistencia legal mutua.

Consideraciones finales

El ciberdelito enfrenta al mundo con un problema que ninguna nación ha tenido que abordar en el pasado, esto es, la permeabilidad de todas las fronteras nacionales. Así, a menos que se tomen medidas urgentes para garantizar que todos los gobiernos del mundo tengan un mínimo de capacidad para responder a las ciberamenazas, todas las naciones sufrirán. Sin embargo, no importa cuán desafiantes y complejos sean, los delitos cibernéticos no están

17 Reitano, Oerting y Hunter, "Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce (J-CAT)".

18 Goodman, "International Dimensions of Cybercrime".

19 Sandeep Mittal y Priyanka Sharma, "A Review of International Legal Framework to Combat Cybercrime", International Journal of Advanced Research in Computer Science 8, n.° 5 (2017).

20 Farouq al Azzam, "The adequacy of the international cooperation means for combating cybercrime and ways to modernize it", Janus.Net: e-Journal of International Relations 10, N.° 1 (2019): 66-83.

21 Goodman, "International Dimensions of Cybercrime".

más allá del alcance de la sociedad[22].

Por ello, se necesita con urgencia un esfuerzo internacional concertado a través del cual se deben superar los problemas financieros, legales, lingüísticos y de política pública asociados con las investigaciones mundiales de delitos cibernéticos, para que las organizaciones encargadas de hacer cumplir la ley puedan continuar protegiendo al público de amenazas criminales graves y emergentes.

No obstante, la red de cooperación internacional encuentra ciertos obstáculos. Entre los países del mundo hay aquellos cuyas leyes penales sustantivas y cuyas leyes de procedimiento penal aún no están en sintonía con la era digital, o que siguen siendo incompatibles con las de los instrumentos normativos internacionales. La preservación de evidencia digital, la ley procesal que permite el rastreo en tiempo real en múltiples jurisdicciones, acuerdos más generalizados para la asistencia legal mutua y la extradición oportuna son algunas de las áreas que requieren un mayor desarrollo.

Todos los países deben adoptar una política unificada para reducir las deficiencias de seguridad en el tratamiento del crimen organizado en sus diversas formas, especialmente los delitos cibernéticos. Esto debe hacerse mediante el establecimiento de un programa coordinado, desarrollando mecanismos más eficientes y depurando las instituciones de justicia penal durante todas las etapas del proceso, que comienza con la recolección de pruebas y termina con el enjuiciamiento.

Hoy en día, la seguridad y la cooperación judicial se ha convertido en uno de los elementos más importantes de las estrategias nacionales y regionales que unifican los procedimientos prácticos de los órganos ejecutivos y trabajan hacia una estrecha cooperación entre los miembros. Por ello, el Estado y, en particular, la Administración de Justicia de cada país adquiere un imperativo moral impostergable por trabajar de manera conjunta y proactiva para prevenir futuros delitos y proteger a la población mundial de esta nueva amenaza del siglo XXI.

22 Goodman, "International Dimensions of Cybercrime".

Bibliografía

al Azzam, Farouq. "The adequacy of the international cooperation means for combating cybercrime and ways to modernize it". Janus. Net: e-Journal of International Relations 10, n.° 1 (2019): 66-83.

Banco Interamericano de Desarrollo. Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe. Washington: Banco Interamericano de Desarrollo, 2020. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Calderoni, Francesco. "The European legal framework on cybercrime: striving for an effective implementation". Crime, Law and Social Change 54, n.° 5 (2010): 339-357.

Cerezo, Ana, Javier Lopez y Ahmed Patel. "International Cooperation to Fight Transnational Cybercrime", Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007), (2007): 13-27.

Christou, George. "The challenges of cybercrime governance in the European Union". European Politics and Society 19, n.° 3 (2018): 355-375.

Goodman, Marc. "International Dimensions of Cybercrime". En Cybercrimes: A Multidisciplinary Analysis, editado por Sumit Ghosh y Elliot Turrini. Berlín: Springer, 2010.

Mittal, Sandeep y Priyanka Sharma. "A Review of International Legal Framework to Combat Cybercrime". International Journal of Advanced Research in Computer Science 8, n.° 5 (2017).

Reitano, Tuesday, Troels Oerting y Marcena Hunter. "Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce (J-CAT)". The European Review of Organised Crime 2, n.° 2 (2015): 142-154.

Ron, Mario, Walter Fuertes, Marco Bonilla, Theofilos Toulkeridis y Javier Díaz. "Cybercrime in Ecuador, an Exploration, which allows to define National Cybersecurity Policies". 2018 13th Iberian Conference on Information Systems and Technologies (CISTI), (2018):1-7.

Sviatun, Olena, Olga Goncharuk, Chernysh Roman, Olena Kuzmenko y Ihor Kozych, "Combating cybercrime: economic and legal aspects", WSEAS Transactions on Business and Economics 18, n.° 1 (2021):751-762.

PERFIL CRIMINOLÓGICO

UNA APROXIMACIÓN A LAS DIFICULTADES EN LA INVESTIGACIÓN Y PERSECUCIÓN DE LOS CIBERCRÍMENES

RICARDO POSADA MAYA[1]

1 Profesor de Derecho Penal y Constitución y Democracia del Área de Derecho Penal, Procesal Penal y Criminología de la Universidad de los Andes, Bogotá-Colombia. Doctor en derecho por la Universidad de Salamanca, España. Especialista en Derecho penal por la Universidad de Antioquia. El presente artículo se inscribe en la línea de aspectos fundamentales del derecho penal sustantivo y procesal penal del Grupo de Investigaciones en Derecho Penal y Justicia Transicional "Cesare Beccaria" de la Facultad de Derecho de la Universidad de los Andes. Igualmente, se inscribe en el proyecto DER2016-79705R del Observatorio de Criminalidad Organizada Transnacional de la Universidad de Salamanca, España.

Resumen. El artículo analiza las más importantes dificultades sustantivas, materiales y probatorias que enfrentan las autoridades al momento de investigar y juzgar los delitos cometidos utilizando sistemas informáticos, electrónicos o telemáticos. En tal sentido, en primer lugar, se distingue entre los conceptos de cibercrimen y delitos informáticos en sentido amplio, precisando cómo estos protegen de forma diferente los bienes jurídicos tutelados, especialmente, las funciones informáticas referidas a la confidencialidad, la integridad, la disponibilidad y el no repudio de los datos y la información susceptible de ser tratados mediante sistemas de información. En segundo lugar, se desglosan los diferentes inconvenientes que permiten llevar a cabo una investigación digital adecuada. Entre las dificultades mencionadas, llaman la atención la falta de conceptos uniformes y claros en la materia, la carencia de estudios estadísticos y criminológicos sobre los mercados del cibercrimen, la ausencia de medios e instrumentos tecnológicos para enfrentarlo, la ausencia de políticas criminales regionales para combatir las organizaciones criminales que utilizan la tecnología para sus delitos, entre otros inconvenientes relacionados con la falta de planeación de las investigaciones y las técnicas para la obtención de evidencia digital que permita demostrar estos delitos. En definitiva, se plantea una aproximación de los principales retos para reducir la impunidad en los delitos tecnológicos.

Palabras claves: Cibercrimen; Delitos informáticos; Evidencia digital; Persecución penal; Datos e información.

Sumario: 1. Aspectos preliminares; 2. Dificultades para combatir de manera adecuada los Cibercrímenes; 3. Conclusión; y 4. Bibliografía.

1. Aspectos preliminares

Cuando se piensa los principales obstáculos teóricos y prácticos para llevar a cabo una adecuada investigación, persecución y judicialización (imputación, acusación y juzgamiento) de los cibercrímenes o los delitos informáticos –en sentido amplio– debe concluirse que son inconvenientes generales a nivel de Iberoamérica[1].

No es un secreto que, a partir de la década de los años 80, con la entrada de la tecnología informática y digital a todos los aspectos de la vida social, familiar e individual[2], comenzaron a surgir nuevos riesgos personales y sociales automáticos, anónimos y descentralizados que demandaron el estudio de los delitos informáticos[3], convertidos en un nuevo paradigma de criminalidad. Una necesidad que se ha incrementado de modo sustancial durante la pandemia del Covid-19, debido al modelo virtual que se ha impuesto en nuestra vida cotidiana. Un cambio que sin duda ha incrementado la vulnerabilidad de las personas y las ha hecho dependientes a la tecnología, lo que ha provocado el aumento de la ciberdelincuencia[4], en especial, aquellas conductas punibles que lesionan o ponen en peligro la intimidad personal y el patrimonio económico.

Buenos ejemplos de estas conductas punibles son las estafas realizadas por medios informáticos (ventas fraudulentas en páginas falsas, ofrecimientos engañosos en línea, inversiones o estafas piramidales online, casinos o loterías arregladas, etc.), la transferencia no consentida de activos patrimoniales (incluyendo monedas virtuales o "puntos" de supermercados o aerolíneas), las defraudaciones y el tráfico ilícito de datos personales *(el fishing o la violación de datos)*, los delitos de intrusión o acceso abusivo a los sistema informáticos –piénsese en las intrusiones en plataformas virtuales como Zoom o Microsoft Teams, que han afectado la intimidad de los usuarios educativos–, el mercadeo ilícito de productos a través de internet, los delitos de obstaculización de datos o sistemas informáticos *(sabotajes o denegaciones de servicios informáticos)*, entre otros comportamientos que lesionan de manera grave los bienes jurídicos. De allí que sea necesario promover la adecuada investigación, judicialización y sanción de estos delitos, no solo con el fin de prevenir su comisión futura, sino también para proteger la seguridad de la información, los

1 M. C. R. Ballesteros & J. A. G. Hernández. "Cibercrimen: Particularidades en su investigación y enjuiciamiento/Cybercrime: Particularities in investigation and prosecution", En: Anuario Jurídico y Económico Escurialense, 47, (2014): 209-233; Jason P. Gonzalez; Matthew A. S Gauger, Neal J. Criminal Justice; CASES WITHOUT BORDERS: The Challenge of International Cybercrime Investigations, (Chicago, Tomo 30, N.º 4, 2016), 15-18; Anthony Reyes; Richard Brittson; Kevin O'Shea; David A. Makin; Amber L. Morczek "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice", En: International Journal of Cyber Criminology, Jan-Jun2015, Vol. 9 Issue 1, (2015): 55-119; James Steele. Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors, (Rockland, MA, Syngress, 2007), 194 y ss. http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=211407&lang=es&site=eds-live&scope=site; Shipley, Todd G.; Bowker, Art. Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace, Syngress, 2014. Accessed April 16, 2021. http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=503592&lang=es&site=eds-live&scope=site

2 En general: Enrique, Anarte Borrallo "Incidencias de las nuevas tecnologías en el sistema penal. Aproximación al derecho penal en la sociedad de la información", En: Derecho y conocimiento 1, 2010, pp. 191-257; Informe Explicativo del Convenio contra el Cibercrimen, ETS-185, del Consejo de Europa y el Parlamento Europeo, 1 y ss. v. https://rm.coe.int/16802fa403; Fernando, Miró Llinares, El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio, (Madrid, Marcial Pons, 2012), 231; David S., Wall Cybercrime. The transformation of crime in the information age, (UK, Polity, 2007), 31 y ss.

3 Ricardo, Posada Maya. "Aproximación a la Criminalidad informática en Colombia", en Revista de derecho, comunicaciones y nuevas tecnologías, núm. 2, Cijus-Gecti, Universidad de los Andes, (2006): 15: "Así las cosas, la fenomenología criminal ha variado como secuela del cambio informático global; pues la primera se ha adaptado al segundo, con el efecto previsible de que los mecanismos institucionalizados de regulación de la vida social han transformado –no siempre de manera adecuada– sus propias perspectivas y criterios de imputación. Especialmente el Derecho penal, con el fin de mejorar sus herramientas de prevención, control y sanción. Y ello es así, pues se afirma que las técnicas jurídicas de control tradicionales resultan cada vez menos eficaces –aunque ello sea discutible– para prevenir o someter formas de criminalidad masificadas, especializadas, continuas, lesivas, muy difíciles de descubrir, rastrear y criminalizar; por oposición a la progresiva vulnerabilidad de las víctimas y de las funciones protegidas".

4 Según el Balance Cibercrimen. (2020). Caivirtual Policia. Recuperado el marzo de 2020, de Centro cibernético policial de Colombia: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf, durante el período entre el 2019 y el 2020, el cibercrimen aumentó en Colombia en un 96% (particularmente por la pandemia del Covid-19). Dicho incrmento puede discriminarse frente al período anterior, así: delitos de acceso abusivo a un sistema informático (94%), suplantación de identidad digital o de sitios Web para la captura de datos personales (377%), violación de datos personales y tráfico ilícito de datos (185%), defraudaciones económicas y transferencias no consentidas de activos (103%), entre otros.

datos y las infraestructuras informáticas críticas[5].

Sin embargo, a pesar de los notables esfuerzos jurídicos y técnicos que han hecho los países de América Latina para combatir el cibercrimen y adecuar sus ordenamientos jurídicos[6], lo cierto es que la cifra oculta de esta clase de criminalidad y la impunidad siguen siendo la regla general en nuestras sociedades. En parte, ello se debe a la falsa creencia de seguridad que tienen las personas de los dispositivos informáticos que utilizan y por la falta de cultura en ciberseguridad y seguridad digital, particularmente, por parte de los sectores más vulnerables a estos delitos, como las pequeñas empresas o los ciudadanos.

2. Dificultades para combatir de manera adecuada los cibercrímenes.

En este contexto, se plantean siete causas que afectan de manera clara la lucha contra el cibercrimen, así:

La primera causa es, justamente, que los encargados del sistema de justicia penal no siempre saben distinguir entre los delitos informáticos (en sentido amplio) y los cibercrímenes. Incluso, sectores importantes de la doctrina y la jurisprudencia le restan importancia a esta distinción teórica y la simplifican, con indeseables consecuencias jurídicas y teóricas[7].

En este sentido, es usual advertir que se promueven definiciones generales con la finalidad de abarcar como delitos informáticos en sentido estricto, todos aquellos delitos comunes que han sido realizados utilizando medios informáticos, electrónicos o telemáticos; o aquellas conductas punibles que pretendan lesionar o poner en peligro las infraestructuras informáticas, como medio y como fin. Todo indica que esta definición general resulta anacrónica, no solo porque impide considerar de manera adecuada las verdaderas características técnicas y jurídicas del cibercrimen, sino además porque desconoce la evolución que han tenido estas figuras en las últimas décadas, por cuenta de los avances tecnológicos que han comenzado a transformar la teoría del delito[8].

A. En realidad, los cibercrímenes son delitos especiales[9] que tienen la función de proteger el bien jurídico tutelado de la seguridad de la información y los datos en formatos electrónicos o informáticos[10] y los sistemas informáticos[11] durante su acceso, procesamiento automático y transmisión eficaz. De manera precisa, buscan proteger las funciones informáticas, es decir, la disponibilidad (o capacidad de uso y tratamiento), la integridad y la confidencialidad (calidad, pureza, idoneidad y corrección) de los datos, la información y las infraestructuras y sistemas informáticos (compuestos por *hardware y software*[12]); además, garantizar a los usuarios el no repudio de sus mensajes y la capacidad de buscar datos específicos en los sistemas de almacenamiento de sus equipos e infraestructuras[13].

A modo de ejemplo, cuando una persona adquiere un dispositivo móvil o una computadora no solo adquiere los servicios que ofrece el dispositivo, sino que también busca la protección de los datos contenidos en él y la defensa de su confidencialidad. Igualmente, se protege su disponibilidad, es decir, que el ciberusuario pueda acceder según su conveniencia –de manera directa o remota– a un equipo conectado a redes de telecomunicaciones y usar o tratar la información almacenada allí, sin ninguna clase de obstáculo o impedimento grave, ilegítimo o no consentido.

Por supuesto, para el ciberusuario es fundamental que el sistema informático, los datos y la información permanezcan íntegros y funcionen en todo momento de manera correcta, sin ser vulnerados de manera violenta o abusiva por parte de terceros que pretendan modificarlos, manipularlos o disminuir su calidad con el propósito de lesionar otros bienes jurídicos como la intimidad personal. Finalmente, es importante garantizar que el sujeto conserve la capacidad de buscar información en el dispositivo o en la nube, ante la enorme cantidad de información que se conserva en estos medios. La seguridad de todas estas situaciones garantiza de manera adecua-

5 En general, Edward G. Amoroso Cyber Attacks: Protecting national infrastructure, (Burlington, Butterworth-Heinemann, 2011); Kenneth Geers "The Cyber Threat to National Critical Infraestructures: Beyond Theory", En: Information Security Journal: A Global Perspective, Jan2009, Vol. 18 Issue 1, (2009): 1-7. DOI: 10.1080/19393550802676097.

6 En relación con los esfuerzos comparados que ha realizado el Ecuador, frente a los demás países de la región, vale la pena revisar el Reporte de Ciberseguridad 2020 del Bid y la OEA, sobre los Riesgos, avances y el camino a seguir en América Latina y el Caribe, que puede consultarse en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

7 Sin embargo, la distinción entre estos delitos y los cibercrímenes se puede advertir con claridad en el Informe Explicativo del Convenio contra el Cibercrimen, § 79, al señalar que los artículos 7 a 10 del Convenio de Budapest se refieren a "(…) delitos comunes que se cometen frecuentemente mediante la utilización de un sistema informático"; también: v. Consejo Nacional de Política Económica y social (Conpes), Documento n.º 3858, 11 de abril de 2016, Bogotá. En línea: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

8 Ricardo, Posada Maya "El Cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual", En: Revista Nuevo Foro Penal, Vol. 13, n. ˚ 13, enero-junio, Medellín, Universidad EAFIT, (2017): 72-112. ISSN 0120-8179.

9 Gustavo Eduardo Aboso y María Florencia Zapata. Cibercriminalidad y derecho penal: la información y los sistemas informáticos como nuevo paradigma, (Montevideo-Buenos Aires, B de F, 2006), 21 y cita 5; Matellanes Rodríguez, "Algunas notas sobre las formas de delincuencia informática en el Código Penal", 130; Ricardo Posada Maya. Los cibercrímenes: Un nuevo paradigma de criminalidad. Un estudio del título VII Bis del Código Penal Colombiano, 103 y 104, dice que son "[…] aquellos comportamientos ilícitos que se dirigen a la indebida creación, procesamiento, almacenamiento, adquisición, transmisión, divulgación, daño, falsificación, interceptación, manipulación previa o posterior, y ejecución automática de datos o sistemas informáticos sin el consentimiento o con abuso del mismo. La finalidad usual de estos comportamientos es lesionar o poner en peligro de manera ilícita […] la seguridad de las funciones informáticas […]". Agrega Posada Maya, "Aproximación a la Criminalidad informática en Colombia", 13-60 (19-20): "[…] no se trata de delitos comunes sino de tipologías especiales realizadas a través de procedimientos informáticos, que gozan de cierta riqueza técnica, aunque no abandonan los tipos penales ordinarios como referentes dogmáticos y criminológicos"; Enrique Rovira Del Canto. Delincuencia informática y fraudes informáticos, Estudios de Derecho penal No. 33, (Dir.) Carlos María Romeo Casabona, (Comares, Granada, 2002),130 y 187; Fernando Velásquez Velásquez, "Criminalidad informática y derecho penal: Una reflexión sobre los desarrollos legales colombianos", En: Derecho penal y nuevas tecnologías. A propósito del título VII bis del Código Penal, Memorias 4, Fernando Velásquez Velásquez, Renato Vargas Lozano, Juan David Jaramillo Restrepo (Comp.), (Bogotá, Universidad Sergio Arboleda, 2016), 353-382 (355).

10 La Convención sobre el Cibercrimen, Budapest 23 de Noviembre de 2001, define los datos informáticos en el capítulo 1, artículo 1, literal b, de la siguiente manera: "(…) se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función", V. https://www.boe.es/eli/es/ai/2001/11/23/(1)/dof/spa/pdf. De manera similar lo hace la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de Europa del 12.07.2013, artículo 2, lit. c), se entiende por dato informático "(…) toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función". V. https://www.boe.es/doue/2013/218/L00008-00014.pdf V. igualmente, Informe Explicativo del Convenio contra el Cibercrimen, § 25.

11 La Convención sobre el Cibercrimen, Budapest 23 de Noviembre de 2001, define los sistemas informáticos en el capítulo 1, artículo 1, literal a, como "(…) todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa". Por su parte, la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de Europa del 12.07.2013, artículo 2, literal a), se entiende por sistema de información: "todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento".

12 Aclara el Informe Explicativo del Convenio contra el Cibercrimen, § 23, que "[…] A los efectos de este Convenio, un "sistema informático" es un dispositivo que consta de hardware y software cuya función es el tratamiento automatizado de datos digitales. Puede incluir facilidades de entrada (input), salida (output) y almacenamiento. Puede funcionar en forma independiente o estar conectado a una red con otros dispositivos similares. "Automatizado" significa sin intervención directa de un ser humano; "tratamiento de datos" significa que los datos que se encuentran en un sistema informático son operados mediante la ejecución de un programa informático. Un "programa informático" es un conjunto de instrucciones que pueden ser ejecutadas por el equipo para alcanzar el resultado deseado. Un equipo puede ejecutar diversos programas. Un sistema informático por lo general consta de diferentes dispositivos, diferenciándose entre el procesador o unidad de procesamiento central y los periféricos. Un "periférico" es un dispositivo que realiza ciertas funciones específicas interactuando con la unidad de procesamiento, como puede ser una impresora, una pantalla de video, un dispositivo para leer o escribir CD u otros dispositivos de almacenamiento de datos" (énfasis propio).

13 Wall, Fighting computer crime, A new framework for protecting information, EE.UU. Wiley, 1998), 120 y Ricardo, Posada Maya, Aproximación a la criminalidad informática en Colombia, (Medellín, Universidad EAFIT, 2017), 22 y ss.; Ricardo, Posada Maya. "¿Puede ser el cibercrimen un delito transnacional?", En: Temas de Derecho penal económico y patrimonial, (Medellín, Universidad Pontificia Bolivariana, 2018), 217-251 (235 a 240). ISBN. 978-958-764-251-7; Rovira del Canto, Delincuencia informática y fraudes informáticos, 65 y ss., 72, 130 y 131; id, "Hacia una expansión doctrinal y fáctico del fraude informático", 118; Id, Los cibercrímenes, 120 a 122; Ricardo Posada Maya "El Cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual", 83.

da la seguridad colectiva e individual de la interacción tecnológica.

Continuando el desarrollo del ejemplo anterior, en el supuesto de que un criminal envíe un correo electrónico infectado con un virus malicioso a otra persona, con el propósito de dañar o deteriorar a un sistema informático y borrar, falsificar o destruir sus datos, se podría configurar una conducta punible de ataque a la integridad de sistemas informáticos (artículo 232) o de falsedad informática (artículo 415, mod. Ley No. 2002-67, artículo 61[14]), con efectos virtuales que no existirán en el mundo físico o analógico causados por medio de instrucciones operativas que se dan durante un procedimiento tecnológico.

Otros buenos ejemplos de cibercrímenes en el Código Orgánico Integral Penal, que se valen de procedimientos de manipulación de sistemas[15], son los delitos de apropiación fraudulenta por medios electrónicos y de telecomunicaciones (COIP, artículo 190; Ley No. 2002-67, artículo 61) que consisten en procurar la transferencia no consentida de bienes valores o derechos en perjuicio de terceros, "alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones"; y el delito de transferencia o apropiación electrónica de activo patrimonial (COIP, artículo 231), cuando el sujeto activo del tipo penal "altere, manipule o modifique el funcionamiento del programa o sistema informático o telemático", para obtener beneficios con ánimo de lucro.

Como se puede apreciar, estas conductas punibles tienen una estructura jurídica particular[16]. Por ejemplo, se realizan de manera automatizada en un ámbito virtual deslocalizado –sin límites físicos precisos–, lo que permite redefinir instituciones dogmáticas como el nexo de causalidad en sentido ontológico, o replantear la estructura tradicional del dolo basada en el conocimiento actual y presencial de la conducta con relevancia jurídico–penal. Más allá, dicha noción implica actualizar los límites de los riesgos programables y su desaprobación jurídica en el mundo virtual y tecnológico que, por cierto, no parecen idénticos a los que se analizan en la imputación objetiva tradicional en el mundo físico, regulados por la normativa nacional o por reglas de práctica profesional *(lex artis, etc.)*. Así mismo, los avances tecnológicos en el derecho moderno exigen revisar igualmente teorías como la participación de personas en la conducta punible, dispositivos amplificadores del delito como la tentativa o causales de ausencia de responsabilidad penal como el error o el consentimiento, que no parece posible seguirlas aplicando sin modificaciones técnicas importantes en esta clase de (ciber)delitos.

Finalmente, teniendo en cuenta que los ataques cibercriminales son verdaderas cadenas de ataques o amenazas informáticas que en algunos ordenamientos jurídicos cubren el reconocimiento de vulnerabilidades (como acto preparatorio), el acceso no consentido a todo o parte del sistema y la obtención ilícita de privilegios virtuales que permitan la realización de ataques (sabotajes, espionaje, etc.) es fundamental que las normas penales le permitan al intérprete delimitar cuidadosamente la posible aplicación concursal de estos comportamientos y evitar desconocer el postulado de non bis in ídem. Usualmente, esto sucede cuando se imputan cargos por el delito medio de acceso abusivo a un sistema informático y, simultáneamente, el delito fin de transferencia informática de activos patrimoniales, pues se desconoce el principio de subsidiariedad material. La importancia de delimitar este tema redundaría, entonces, en la precisión de las imputaciones de cargos y en los pliegos de acusación fiscales en nuestro medio.

14 Convención sobre el Cibercrimen, artículo 4. º (Interferencia de datos); Informe Explicativo del Convenio contra el Cibercrimen, §§ 60 y ss. En cuanto a la integridad del sistema, ibíd., §§ 65 y ss.

15 Convención sobre el Cibercrimen, artículo 8. º (Fraude informático); Informe Explicativo del Convenio contra el Cibercrimen, §§ 86 y ss.

16 Posada Maya, "Los cibercrímenes", 207 – 216; Posada Maya, "El cibercrimen y sus efectos en la teoría", 84 - 88.

B. Por el contrario, los delitos informáticos en sentido amplio[17] son aquellas conductas punibles que pueden ser realizadas mediante el empleo de medios informáticos, electrónicos o telemáticos. Sin embargo, dicha forma de comisión es solo circunstancial y no hace parte de la definición del tipo penal fundamental. Sería el caso, por ejemplo, un delito de estafa (COIP, artículo 186) realizado mediante el empleo de un correo electrónico para engañar a los sujetos pasivos (simulación de hechos falsos o deformando u ocultando hechos verdaderos) y obtener de ellos un provecho patrimonial ilícito, que sigue siendo un delito económico común. Así, esta conducta de ingeniería social solo protege de forma residual la seguridad de la información, los datos y los sistemas informáticos.

La naturaleza de este delito tampoco cambia a una especial cuando su comisión esté precedida del "uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares" (COPI, inciso 2.º *ibíd.*). En estos casos, el incremento de la pena se justificaría por el uso de esta clase de instrumentos que facilitan la ejecución del delito y dificultan la defensa de la víctima (mayor desvalor de acción objetivo).

Por tal motivo, a pesar de que los cibercrímenes y los delitos informáticos –en sentido amplio– son estructuras jurídicas que comparten algunos elementos típicos, todo indica que conservan su propia naturaleza y protegen con diferente prioridad los bienes jurídicos tutelados.

La segunda causa que obstaculiza la persecución y sanción de la cibercriminalidad en nuestro medio es que las autoridades usualmente califican los cibercrímenes (en términos jurídicos y estadísticos) con base en simples criterios formales, esto es, por el solo hecho de estar previstos de esa manera en la legislación penal (COIP)[18]. Una postura que carece de criterios materiales y que resulta problemática por las siguientes razones:

De un lado, desconoce las consecuencias que tiene esta distinción teórica en la práctica judicial. Es conveniente destacar que los cibercrímenes son realizados mediante instrucciones informáticas programadas en un mundo virtual (deslocalizado y desregulado) por un ciberusuario (con identidad física y digital) y ejecutadas por un sistema informático conectado a la red. No son delitos realizados por sujetos mediante acciones físicas en un mundo analógico como unas lesiones personales o un hurto con arrebato de la cosa. El solo hecho de que estas conductas sean

17 Citas de delito informático en sentido Amplio: José Luis, De La Cuesta Arzamendi (Dir.) /Norberto J. De La Mata Barranco (Coord.). Derecho penal informático, (Madrid, Civitas-Thomson Reuters, 2010), 31 y 159; Alfonso, Galán Muñoz, El fraude y la estafa mediante sistemas informáticos: análisis del artículo 248.2 C.P., (Valencia, Tirant lo Blanch, 2005), 29 y ss.; Nuria, Matellanes Rodríguez, "Algunas notas sobre las formas de delincuencia informática en el Código penal", En: Hacia un Derecho penal sin fronteras, Coord. María Rosario Diego Díaz-Santos y Virginia Sánchez López, XII Congreso Universitario de Alumnos de Derecho penal, (Madrid, Colex, 2000), 129-147 (130); Miró Llinares, El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio, 33 y ss.; Laura, Mayer Lux "Defining cyberterrorism", En: Revista Chilena de derecho y tecnología, vol. 7, núm. 2, (2018), 5-25 (13). Doi 10.5354/0719-2584.2018.51028; Ricardo Posada Maya, Los cibercrímenes: Un nuevo paradigma de criminalidad. Un estudio del título VII Bis del Código Penal Colombiano, 101-102; Helmut, Satzger, "La protección de datos y sistemas informáticos en el derecho penal alemán europeo. Tentativa de una comparación con la situación legal en Colombia", En: Derecho penal y nuevas tecnologías. A propósito del título VII bis del Código Penal, Memorias 4, Fernando Velásquez Velásquez, Renato Vargas Lozano, Juan David Jaramillo Restrepo (Comp.), (Bogotá, Universidad Sergio Arboleda, 2016), 11 y ss. (12); Ulrich, Sieber, Computerkriminalität und Strafrecht. Neue Entwicklungen in Technik und Recht, 2a ed., (Köln-Berlin-Bonn-München, Heymanns, 1980), 39; Klaus, Tiedemann. "Criminalidad mediante computadoras", trad. de Amelia Mantilla viuda de Sandoval, En: Nuevo Foro Penal No. 30, octubre–diciembre de 1985, (Bogotá, Temis), 481 a 492; Unión Internacional de Telecomunicaciones (UIT/ITU). Understanding Cybercrime: phenomena, challenges and legal response, Ginebra, UIT, 2012, 11. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf; Wall, "Criminalizing cyberspace: the rise of the Internet as a 'crime problem'", 22-103. En general: Alberto, Suárez Sánchez. Manual de delitos informático en Colombia. Análisis dogmático de la ley 1273 de 2009, (Bogotá, Universidad Externado de Colombia, 2016).

18 Dicho criterio formal ha sido problemático, pues ha permito que algún sector de la doctrina colombiana, por ejemplo, indique el delito de Hurto por medios informáticos, previsto en el C.P. de 2000, artículo 269I, es un cibercrimen, cuando en realidad es un simple delito común de naturaleza patrimonial que puede ser realizado por medio de sistemas informáticos, electrónicos o telemáticos, superando las medidas de seguridad (por manipulación del sistema o por suplantación del usuario legítimo) que permiten el apoderamiento de una cosa mueble ajena. En tal sentido, resulta más coherente el COIP, pues consagra como verdaderos delitos patrimoniales, los delitos de Estafa simple y agravada por copia, hurto, etc. de tarjetas bancarias (artículo 186, inciso 2.º, núm.. 1) y agravado por el uso de dispositivos electrónicos en cajeros bancarios automáticos par alterarlos o para obtener códigos personales (artículo 186, inciso 2.º, núm.. 2). Mientras que dispone de los cibercrímenes en los delitos contra la seguridad de los activos de los sistemas de información y comunicación, a partir de los artículos 229 y ss.

realizadas por ciberusuarios conectados a sistemas informáticos supone una compleja transformación de los presupuestos sustantivos del crimen y de la prueba requerida para superar el estándar de responsabilidad penal (particularmente, para vincular la identidad del usuario digital y el físico en la ejecución del crimen, una vez se ha descartado la existencia de una suplantación durante la conexión de estos con el sistema informático)[19].

Por otro lado, esta postura formal induce a una importante equivocación metodológica que consiste en equiparar las técnicas o los modos de ejecución empleados en los cibercrímenes con los delitos imputables en cada caso. En efecto, una cosa es el delito de violación o interceptación ilegal de datos o uso de herramientas para vulnerar seguridades informáticas u obtener información protegida o secretos (COIP, artículo 230 y Ley No. 2002-67, artículo 58) y otra son las múltiples técnicas informáticas utilizadas por los criminales para interceptar información en su origen o para copiar o clonar información de las tarjetas bancarias, u obtener información que deba permanecer en reserva o secretos. Incluso, estas técnicas informáticas son diferentes a las técnicas populares de engaño para obtener datos personales como el *fishing* o "los ataques de fuerza bruta" para acceder de forma no consentida a sistemas informáticos (COIP, artículo 234). Es cierto que en algunos casos este inconveniente surge debido a una inadecuada traducción o interpretación de la literatura científica, del Convenio contra el Cibercrimen (Budapest), de su reporte explicativo o de la legislación europea o norteamericana, no obstante, en su mayoría estas confusiones son superables.

De igual manera, esta tendencia teórica permite que, al momento de definir los cibercrímenes en la ley, se confundan conceptos como los medios de comunicación, los medios ejecutivos del crimen y las redes sociales, cuando es claro que todos ellos se refieren a ámbitos y contextos diferentes. De este modo, por ejemplo, la red debe entenderse como un medio que permite la interconexión de los sistemas en un mundo virtual, más no como una estructura delictiva autónoma que califique los delitos.

Como se puede apreciar, en este ámbito coexisten una serie de prejuicios y malentendidos teóricos y prácticos que desorientan a los especialistas técnicos y a los estudiosos del derecho penal cuando pretenden definir esta clase de criminalidad. Ello exige una mejor y más clara interacción interdisciplinaria entre la ingeniería de sistemas, la criminología y el derecho penal al momento de desarrollar las diferentes categorías dogmáticas y estudiar con mayor rigor los diferentes bloques o modelos de micro y macro criminalidad y las tendencias ejecutivas que afectan la seguridad de la información, los datos y los sistemas informáticos (electrónicos y telemáticos).

La tercera causa tiene relación con el déficit de estadísticas criminales confiables que reflejen la ocurrencia y los efectos del cibercrimen en nuestras sociedades (efectos económicos, sexuales, de protección de datos, contra la intimidad, violaciones a los derechos morales y patrimoniales de autor, etc.). Este problema también impacta en la calidad de las bases de datos que gestionan los servicios jurídicos, de seguridad e inteligencia del Estado, entre ellos, Policía Nacional y la Fiscalía General del Estado (instituciones que no siempre comparten la información de manera bidireccional). Además, se acepta que la ausencia de cifras o su figuración hace difícil el desarrollo mecanismos de colaboración de información efectivos que permitan crear e implantar en Latinoamérica políticas públicas y criminales que puedan ser verificadas a largo y a corto plazo,

19 Me he referido al tema previamente, Ricardo, Posada Maya, "El Cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual", sobre el concepto de ciber acción: 82 y ss.; sobre el concepto de ciberusuario: 88 y ss. Sobre la suplantación. Cristian Borghello / Marcelo G. I.,Temperini, "Suplantación de identidad digital como delito informático", En: Daniela, Dupuy, (Dir.)/ Mariana, Kiefer (Coord.). Cibercrimen, Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet, (Buenos Aires-Montevideo, BdeF, 2017), 291-311; María Belén, Sánchez Domingo. "Robo de identidad personal a través de la manipulación o el acceso ilegítimo a sistemas informáticos, ¿Necesidad de una tipificación específica?", En: Revista General de Derecho Penal (IUSTEL), No. 26, noviembre de 2016, No. 418038, PDF on-line, España, pp. 1/34. Sankhwar, S., Pandey, D., Khan, R.A. "A Step Towards Internet Anonymity Minimization: Cybercrime Investigation Process Perspective", En: Satapathy S., Tavares J., Bhateja V., Mohanty J. (eds) Information and Decision Sciences. Advances in Intelligent Systems and Computing, vol. 701, (2018), Springer, Singapore. https://doi-org.ezproxy.uniandes.edu.co:8443/10.1007/978-981-10-7563-6_27

o enmendar las que existen a partir de dicha información. Un ulterior efecto es la dificultad para que las agencias estatales puedan desarrollar controles de (ciber)seguridad que permitan la protección eficiente de los intereses públicos y de los derechos ciudadanos.

Este inconveniente también se compondría si nuestros países limitan la existencia de entidades de investigación con funciones de policía judicial paralelas (judiciales, administrativas, ejecutivas, etc.) que duplican de forma innecesaria los esfuerzos para esclarecer los delitos, producen información contradictoria y reducen de manera sustancial los escasos recursos económicos y técnicos que usualmente se destinan a esta materia.

En definitiva, se puede concluir que América Latina aún no cuenta con una definición uniforme y clara sobre la cibercriminalidad –que la distinga de los delitos comunes que pueden ser realizados por medios informáticos–, ni dispone de diagnósticos completos sobre su ocurrencia, sus modalidades y las víctimas más vulnerables[20], ni de protocolos unificados que posibiliten determinar las metodologías de ejecución más empleadas por los criminales[21]. Estas deficiencias teóricas y técnicas también permiten explicar el por qué en nuestras legislaciones penales –más allá de la influencia de los convenios, tratados y directivas internacionales– son tan usuales los trasplantes jurídicos en derecho penal y tecnología que, por cierto, muchas veces hacen invisibles o dependientes los desarrollos y esfuerzos locales para adaptar nuestros ordenamientos jurídicos a la realidad social. No es de extrañar entonces, que esta materia en los códigos penales termina siendo más simbólica que preventiva.

La cuarta causa consiste en las notorias dificultades que se les imponen a las víctimas en nuestro entorno cultural para acceder a la administración de justicia, investigar y denunciar esta clase de delitos virtuales, en particular, tras la aparición de la pandemia del Covid-19. Del mismo modo, a pesar de los ingentes esfuerzos de las autoridades, tampoco se observa en nuestra región una reducción sustancial del plazo razonable entre las denuncias de los posibles cibercrímenes y el comienzo de las investigaciones formales. Todo lo contrario, dicho plazo parece incrementarse con el tiempo, incluso en perjuicio de los actos fiscales urgentes (COIP, artículo 583).

Con esto en mente, la investigación y judicialización de esta clase de comportamientos representa un enorme desafío para los Estados de la región, especialmente, en lo que concierne a las imputaciones y acusaciones de cargos y a la obtención de evidencias y pruebas (digitales). Aquello no solo por las lagunas en la regulación legal que impiden adelantar investigaciones técnicas, sino también porque es frecuente que en el sector privado las empresas de telecomunicaciones o el sistema financiero se impongan restricciones u obstáculos para conocer y tratar su información comercial o financiera, incluso por parte de ciertas entidades del Estado, lo que redunda en una mayor impunidad o en una mayor cifra oculta de criminalidad. Así, se demuestra que estamos frente a un verdadero círculo vicioso que se extiende también a la posibilidad de que las víctimas obtengan directamente dicha información en sus investigaciones privadas, cuando estas estén habilitadas por la ley para hacerlo en modelos procesales de tendencia acusatoria[22].

Adicionalmente, incluso si las compañías que prestan los servicios de información entregan o revelan oportunamente la información solicitada a las autoridades judiciales o las víctimas, no siempre es posible garantizar su calidad o su identidad, entre otras cosas, porque los funcionarios de la policía judicial que adelantan esta clase de diligencias difícilmente la buscan y obtie-

20 Stancu, AI. "Cybercriminals and the Victims of Cybercrime", Journal of Law and Administrative Sciences [s. l.], v. 14, n. 14, (2020), 127–136 http://search.ebscohost.com/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.jladsc14.17&lang=es&site=eds-live&scope=site

21 Rachana Y. Patil; Satish R. Devane "Network Forensic Investigation Protocol to Identify True Origin of Cyber Crime", En: Journal of King Saud University - Computer and Information Sciences, January (2019), DOI: 10.1016/j.jksuci.2019.11.016

22 Sobre la posible investigación de las víctimas: Prunckun, Henry W. Intelligence and Private Investigation: Developing Sophisticated Methods for Conducting Inquiries. Charles C Thomas; 2013, 2 y ss. http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=608003&lang=es&site=eds-live&scope=site

nen directa y personalmente de los sistemas informáticos requeridos (en general, es entregada o enviada por los funcionarios de la entidad requerida) lo que desconoce las reglas usuales de cadena de custodia de evidencia digital.

Para terminar este aparte, es inevitable insistir en mejorar las condiciones materiales y de infraestructura que requieren los protocolos de cadena de custodia para datos o información en formato informático o digital. En particular, aquellas prácticas que, por ejemplo, suponen utilizar el simple correo para el envío de información, la obtención no personal de datos o información, o la manipulación de la evidencia, etc. Prácticas que pueden tener un impacto importante en la valoración de la evidencia digital y en la formación de la convicción del juez, respecto a la identidad de los elementos presentados o incorporados como pruebas al juicio oral[23].

La quinta causa, como desarrollo de la anterior, consiste en la falta de normativa clara sobre las obligaciones de conservación, protección y exhibición de datos informáticos para garantizar las actuaciones urgentes de las autoridades judiciales en los casos de cibercrimen o de delitos informáticos en sentido amplio. Dentro de los temas importantes, se pueden mencionar los siguientes:

A. La conservación de los datos informáticos previamente almacenados por entidades públicas o privadas, especialmente, aquellos referidos al sector bancario o de las telecomunicaciones. Como lo señala la Convención de Budapest, esto tiene la mayor importancia cuando se trata de actividades de investigación en las cuales las autoridades necesitan la conservación rápida de datos informáticos o de información almacenados en sistemas informáticos o lógicos, cuando su naturaleza volátil implique el riesgo de que estos puedan perderse, o cuando puedan ser modificados por terceros de manera ilegítima[24] con grave perjuicio de su custodia (COIP, artículo 500, núm. 2) y del principio de identidad de la prueba en el juicio oral.

En el mismo sentido, debería incluirse la posibilidad de que las autoridades judiciales le puedan ordenar a los particulares –comprendidas las víctimas– conservar, guardar y proteger, durante un tiempo determinado, los datos (reservados o no) que posean en sus sistemas informáticos o en sistemas de almacenamiento lógico, aun si estos no sean de su titularidad[25]. La normativa internacional sugiere que ello se pueda realizar con independencia de que en el tráfico de la información o los datos protegidos o almacenados hayan participado varias personas de manera conjunta, alternativa o secuencial, o múltiples proveedores de servicios de telecomunicaciones[26].

Dichos documentos también proponen que estas facultades se extiendan a la obligación de garantizar –como se ha destacado en la cuarta causa– la obligación de las entidades públicas o privadas de revelar de manera ágil datos informáticos específicos a los agentes de la policía judicial, con el fin de que estos pueden identificar aspectos importantes como los proveedores, los emisores o receptores de comunicaciones previas y los canales por medio de los cuales fue

23 En general, sobre el tema del cibercrimen y la cadena de custodia, Michael, Meek Neira. Delito informático y cadena de custodia, (Bogotá, Universidad Sergio Arboleda, 2013).

24 La Convención sobre el Cibercrimen, Budapest 23 de Noviembre de 2001, artículo 16.1; Informe Explicativo del Convenio contra el Cibercrimen, §§ 149 y ss. La convención distingue entre el hecho de guardar datos almacenados de forma segura y retener o acumular datos a partir de un momento determinado. Justamente, en el § 155, señala: "Por lo tanto, valiosas pruebas de un delito pueden desaparecer fácilmente debido a negligencias en el manejo o las prácticas de almacenamiento; a la manipulación o borrado deliberados de los datos con el fin de destruir las pruebas, o a la eliminación sistemática de datos cuya conservación no se requiere por más tiempo. Un método de preservar la integridad de los datos es que las autoridades competentes registren, o accedan de manera similar, y confisquen, o consigan de manera similar, los datos necesarios. Sin embargo, cuando los datos están bajo la custodia de alguien de confianza, tal como una empresa de renombre, la integridad de los datos puede preservarse más rápidamente con una orden de conservación de datos. Para las empresas legítimas, una orden de conservación de datos puede representar también un menor perjuicio para sus actividades normales y su reputación que el efectuar un registro y confiscación en sus instalaciones". COIP, artículo 476, núm.. 8.

25 La Convención sobre el Cibercrimen, Budapest 23 de Noviembre de 2001, artículo 16.2.

26 La Convención sobre el Cibercrimen, Budapest 23 de Noviembre de 2001, artículo 17.1.a)

tratada la información o los datos por parte de los posibles responsables del delito[27].

B. La presentación o comunicación voluntaria de datos informáticos a las autoridades judiciales. En este caso, la normativa procesal debería permitirle a una persona o a una entidad pública o privada entregar o comunicar de manera voluntaria a las autoridades judiciales datos informáticos de su titularidad o de terceros –que este posea, controle o haya almacenado previamente, etc. –, de los cuales se pueda inferir la posible comisión de un cibercrimen o de un delito informático en sentido amplio. La normativa internacional recomienda que la información también incluya los datos de los clientes anteriores que estos hayan incluido en el tráfico electrónico o que puedan dar pistas de su navegación en internet, así como los datos de los usuarios, su posible localización, los datos de los dispositivos utilizados, incluyendo los números de identificación y de conexión IP, información contractual, financiera y de facturación de los servicios, etc.[28].

C. Otras medidas o actividades que permitan la investigación cibercriminal. De igual forma, los documentos mencionados aconsejan reglamentar diferentes medidas de investigación, entre las cuales vale la pena destacar las siguientes[29]:

1. Búsquedas y registros selectivos de datos informáticos en bases de datos públicas o privadas (reservadas), sistemas de almacenamiento de información o sistemas informáticos, cuando estos estén relacionados con la posible comisión de una conducta punible. Tales facultades deberían permitirles a las autoridades mecanismos ágiles para obtener la extensión de la búsqueda a otros sistemas o medios de almacenamiento que resulten vinculados o conectados con los datos registrados previamente[30] (por ejemplo, correos electrónicos).

Estas medidas deberían mejorar las operaciones encubiertas (COIP, artículo 483) realizadas por agentes encubiertos en operaciones digitales.

2. La confiscación, copia y conservación confidencial e íntegra de los datos obtenidos con fines judiciales en los procedimientos de búsqueda o registro; y confiscación o copia de dispositivos de almacenamiento lógico o de sistemas informáticos como computadores o teléfonos móviles, entre otros[31]. Medidas que se integrarían con aquellas cautelares ordinarias y las que permite adoptar el COIP, artículo 494, para efectos de la cooperación eficaz con otros Estados de la región.

27 La Convención sobre el Cibercrimen, Budapest 23 de Noviembre de 2001, artículo 17.1.b); Informe Explicativo del Convenio contra el Cibercrimen, §§ 165 y ss. Se agrega a § 166, que: "La obtención de los datos relativos al tráfico almacenados correspondientes a comunicaciones pasadas puede ser esencial para determinar el origen o el destino de las comunicaciones realizadas, elemento crucial para identificar a las personas que han distribuido, por ej., pornografía infantil, información fraudulenta como parte de un plan fraudulento o virus informáticos, o que han intentado acceder o han accedido ilegalmente a sistemas informáticos, o que han transmitido comunicaciones a un sistema informático causando interferencias, ya sea a los datos contenidos en el sistema o a su correcto funcionamiento".

28 La Convención sobre el Cibercrimen, Budapest 23 de noviembre de 2001, artículo 18; Informe Explicativo del Convenio contra el Cibercrimen, §§ 170 y ss.

29 En general, Daniela, Dupuy (dir.); Mariana, Kiefer (coord.). Cibercrimen: aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet; prólogo de Germán C. Garavano; presentación Luis J. Cevasco, B de f; (Buenos Aires, Euros Editores, 2016); Daniela, Dupuy (dir.); Mariana, Kiefer (coord.). Cibercrimen II: nuevas conductas penales y contravencionales, inteligencia artificial aplicada al derecho penal y procesal penal, novedosos medios probatorios para recolectar evidencia digital, cooperación internacional y victimología; prólogo Marcos Salt, (Buenos Aires: B de F, 2018).

30 La Convención sobre el Cibercrimen, Budapest 23 de Noviembre de 2001, artículo 19; Informe Explicativo del Convenio contra el Cibercrimen, §§ 184 y ss.

31 La Convención sobre el Cibercrimen, Budapest 23 de Noviembre de 2001, artículo 19.

3. Eliminar los datos originales o información encontrados en los registros selectivos en sistemas informáticos o medios de almacenamiento lógico cuando estos puedan poner en peligro la seguridad o los derechos fundamentales de personas, o la seguridad de entidades o del Estado (por ejemplo, piénsese en material sexual con menores de edad, documentos oficiales secretos o reservados, información sensible o privada de las personas, etc.)[32].

4. Interceptar canales, obtener o grabar datos informáticos por medios técnicos en su territorio, sea a través de sus agencias judiciales o con la asistencia de entidades que presten servicios de telecomunicaciones, con el fin de esclarecer delitos graves. La idea es que la obtención de información o datos se dé durante su tráfico mediante la interceptación de aquellos canales que permiten las comunicaciones transmitidas por sistemas informáticos, o que sean obtenidos durante su proceso de almacenamiento. Lo dicho incluye la obligación de mantener en reserva dichas actividades y los resultados de la búsqueda[33].

En fin, como estas actividades de investigación complejas afectan derechos constitucionales fundamentales como la intimidad, el debido proceso, el derecho de defensa, el derecho a la no autoincriminación o pueden lesionar derechos de terceros de buena fe, es imprescindible que la ley procesal penal disponga de los respectivos controles judiciales –previos y/o posteriores– para garantizar que las actividades resulten ajustadas a la ley y a los tratados internacionales, necesarias, proporcionales y razonables en el marco de una investigación judicial de interés público[34].

La sexta causa radica en los inconvenientes relacionados con la prueba técnica informática o digital, la investigación de la escena digital y con la falta de planificación de las investigaciones sobre cibercrimen[35]. En este sentido, se pueden mencionar varias deficiencias importantes, que deben ser corregidas por nuestros ordenamientos procesales.

A. El desconocimiento de los agentes de la policía judicial o de la fiscalía en cuanto a la obtención o recuperación estándar, aducción, aseguramiento y exhibición –con cumplimiento de la cadena de custodia– de aquella evidencia digital[36] o medio probatorio en formato informático o digital que puede ser reconocido (auditada y trazable[37])

32 La Convención sobre el Cibercrimen, Budapest 23 de Noviembre de 2001, artículo 19.

33 La Convención sobre el Cibercrimen, Budapest 23 de Noviembre de 2001, artículos 20 y 21; Informe Explicativo del Convenio contra el Cibercrimen, §§ 205 y ss.; §§ 216 y ss. En el § 209 se afirma: "Se pueden obtener dos tipos de datos: los datos relativos al tráfico y los datos relativos al contenido. De acuerdo con la definición del artículo 1.d se entiende por "datos relativos al tráfico" todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente. En el Convenio no se define el término "datos relativos al contenido", pero este se refiere al contenido comunicativo de la comunicación, es decir, el significado o la finalidad de la comunicación, o el mensaje o información transmitidos por la comunicación (excepto los datos relativos al tráfico)".

34 Informe Explicativo del Convenio contra el Cibercrimen, §§ 146 y ss.

35 Learner, D. E. Electronic Crime Scene Investigation, New York, Nova Science Publishers Inc; 2009. http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=311082&lang=es&site=eds-live&scope=site; Albert J, Marcella; Frederic, Guillossou. Cyber Forensics: From Data to Digital Evidence, (New Jersey, Wiley, 2012), 207 y ss.

36 Fredy, Bautista García; Álvaro José, Mosquera Suárez; Andrés, Meneses Obando y Daniel Ríos Sarmiento. Evidencia Digital. Aspectos generales, Rama Judicial, Consejo Superior de la Judicatura, Escuela Judicial Rodrigo Lara Bonilla, (Bogotá, 2020), 7 y ss.

37 S. M. Nirkhi, R. V. Dharaskar and V. M.Thakre, "Analysis of online messages for identity tracing in cybercrime investigation," Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), (Kuala Lumpur, Malaysia, 2012), 300-305, doi: 10.1109/CyberSec.2012.6246131.

como prueba en los juicios, en relación con los delitos realizados en entornos o con medios virtuales. Al margen de lo anterior, debe existir amplia regulación de los mensajes de datos almacenados en dispositivos tecnológicos y lógicos que puedan ser declarados admisibles como medios de prueba en la legislación interna, conforme a los estándares ISO internacionales.

Por lo demás, ello exige que la autoridad competente regule de forma clara y precisa, a través de protocolos, las técnicas digitales forenses específicamente admitidas para enfrentar las diferentes características de la evidencia digital (volátil, eliminable, duplicable, anónima, alterable y modificable)[38]. Esto, además, para garantizar que las actividades de investigación respetan y cumplen con los diferentes requisitos legales para considerarla legal, lícita, creíble, admisible, auténtica, completa y confiable[39]. No basta con una somera mención de dichas características en la ley, es necesario desarrollarlas para que todos puedan entender sus alcances y las limitaciones que se desprenden de ellas.

B. La falta de programas metodológicos serios que permitan planificar adecuadamente el diseño de la búsqueda, recolección, obtención, preservación, embalaje, etc. de la prueba digital necesaria para demostrar los cibercrímenes en el juicio. En otras palabras, para garantizar la práctica adecuada de la prueba y su análisis técnico–científico. Ello es particularmente importante cuando se trata de casos que afectan la seguridad o la defensa nacional[40].

Naturalmente, para que la planificación de la investigación judicial pueda ser exitosa es primordial que las actividades judiciales estén precedidas por aproximaciones interdisciplinarias y colaborativas, que utilicen de manera correcta los diferentes términos técnicos y jurídicos en las diferentes etapas de una investigación digital forense. En dichas actividades de colaboración se deben seguir de manera estricta los diferentes deberes de actuación para no producir inconvenientes innecesarios[41]. Así, por ejemplo, los líderes técnicos de la investigación deben ser principalmente ingenieros, mientras que los líderes que impulsan la imputación de cargos y la acusación de los posibles autores deberán ser abogados especializados.

C. También es importante anotar que las entidades del Estado encuentran importantes obstáculos en la falta de iniciativas y desarrollo en legal tech, especialmente, de equipos y software especializados, licenciados y autorizados –con código abierto– para adelantar toda clase de investigaciones o pesquisas judiciales efectivas. La carencia de estos medios implica que, en muchos casos, la actividad de investigación no se ajuste a los estándares legales o internacionales en materia de identidad y seguridad de la evi-

38 Nirkhi, Dharaskar and Thakre, "Analysis of online messages for identity tracing in cybercrime investigation", 46 - 48. Cano Martínez, Jeimy. Computación forense: descubriendo los rastros informáticos, 2ª ed., Bogotá, Alfaomega, 2015, 109 y ss.; Cross, Michel. Scene of the Cybercrime, 2.ª ed., Burlington, Syngress, 2008, 201-242; Da-Yu, Kao; Ni-Chen, Wu; Fuching, Tsai. "The Governance of Digital Forensic Investigation in Law Enforcement Agencies", 21st International Conference on Advanced Communication Technology (ICACT), (PyeongChang, South Korea, 2019), 61-65, doi: 10.23919/ICACT.2019.8701995; Kyung-Shick Choi, Toro-Álvarez, Marlon Mike. Cibercriminología: guia para la investigación del cibercrimen y mejores prácticas en seguridad digital= Cybercriminology: guide for cybercrime investigation and best practices in digital security, (Bogotá: Universidad Antonio Nariño; Boston MA: Boston University, 2017), 20 y ss.

39 Bautista García; Mosquera Suárez; Meneses Obando; y Ríos Sarmiento, "Evidencia Digital. Aspectos generales", 48 - 50.

40 M, Eckenwiler; S. McCulloch National Security Cyber Investigations: Considerations and Challenges. United States Attorneys' Bulletin [s. l], v. 67, n. 1, (2019), 43–64,. http://search.ebscohost.com/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.usab67.8&lang=es&site=eds-live&scope=site

41 Peter M. Bednar; Vasilios, Katos; Cheryl. Hennell "On the Complexity of Collaborative Cyber Crime Investigations", En: Digital Evidence and Electronic Signature Law Review, Vol. 6, (2009): 214-219.

dencia digital, además de hacer muy dispendiosa (y costosa) la obtención y disposición de múltiples versiones de software licenciado que le permitan realizar las correspondientes comparaciones y averiguaciones técnicas de la evidencia, a partir del software empleado efectivamente por los cibercriminales.

D. Las malas prácticas al momento de producir la prueba en el proceso. Uno de los fenómenos más comunes en el ámbito de las investigaciones digitales es la falta de selección de la evidencia obtenida, exhibida y solicitada como prueba en el juicio oral (o en las audiencias públicas correspondientes), que luego no se practica en su totalidad por la renuncia expresa de alguna de las partes procesales. Así mismo, el solo hecho de que las contrapartes tengan que revisar grandes volúmenes de evidencia e información que se descubre de manera innecesaria en los procedimientos judiciales, sin ninguna clase de control previo de material, produce una quiebra del plazo razonable del proceso judicial y afecta de manera tangible los derechos de defensa y contradicción, así como en la eficacia del juicio y en la inmediación del juez.

E. Para terminar este aparte, es necesario evitar la alta rotación de funcionarios judiciales o de investigación entre las diferentes entidades del Estado. Rotación que no solo permite una dispersión injustificada de las distintas investigaciones judiciales, sino también que se desperdicien las capacitaciones especializadas a funcionarios judiciales y agentes fiscales y, con ello, la oportunidad de hacer investigaciones realmente eficaces. Es inconcebible que dichos funcionarios sean reemplazados por personas que desconocen las técnicas de investigación o el lenguaje técnico aplicado.

Finalmente, la séptima causa es que muchos de los cibercrímenes (ciber lavado, ciber terrorismo, narcotráfico por medios informáticos, pornografía, etc.) más graves en la región no están regulados de manera similar por los Estados que deben enfrentarlos conjuntamente[42]. Indudablemente, tales crímenes no pueden ser investigados o perseguidos de forma insular, sobre todo, cuando tienen alcances o repercusiones transnacionales. La situación precisa de una mejor armonización de la normativa penal internacional y regional en el ámbito de la cibercriminalidad organizada transnacional[43].

Cabe agregar la necesidad de explorar y conocer, desde una perspectiva criminológica, las distintas formas de macro y micro criminalidad relacionadas con el internet que tiene especial repercusión en América Latina, como por ejemplo, el narcotráfico y el lavado de activos, la venta de armas y de órganos humanos, los delitos de explotación sexual, pornografía infantil[44], financiaciones ilícitas, el terrorismo y, en general, aquellos mercados criminales que son liderados

42 Sobre los efectos transnacionales del cibercrimen, Abraham D.Sofaer, / Seymour E. Goodman "Cyber Crime and Security. The transnational dimension", En: Hoover Press, Cyber, SF, (Stanford University: California, 2013), 6 y ss. En : http://media.hoover.org/sites/default/files/documents/0817999825_1.pdf

43 Convención de las naciones unidas contra la delincuencia organizada transnacional y sus protocolos (En adelante, Convención de Palermo), oficina de las naciones unidas contra la droga y el delito, Nueva York, Naciones Unidas, 2004, https://www.unodc.org/pdf/cld/TOCebook-s.pdf; Resolución AG/RES. 2026 (XXXIV-O/04) contra la Delincuencia Organizada Transnacional en el Hemisferio, aprobada en la cuarta sesión plenaria de la Organización de Estados Americanos (OEA), celebrada el 8 de junio de 2004: http://www.oas.org/juridico/spanish/ag04/agres_2026.html; Ricardo, Posada Maya "¿Puede ser el cibercrimen un delito transnacional?", 217-251; Laura, Zúñiga Rodríguez, Criminalidad organizada y sistema de derecho penal. Contribución a la determinación del injusto penal de organización criminal, (Granada, Comares, 2009), 6 y ss.; Laura, Zúñiga Rodríguez, "El concepto de criminalidad organizada transnacional: problemas y propuestas", En: Revista Nuevo Foro Penal, Vol. 12, No. 86, enero-junio 2016, (Universidad EAFIT, Medellín, 2016): 62-114.

44 Gonzalo, Quintero Olivares. "Problemas de la perseguibilidad de los ciberdelitos". En: Ciberdelitos. Grooming – Stalking – Bullying – Sexting – Ciber odio – Propiedad intelectual – Problemas de perseguibilidad –Ciberpornografía infantil, Marcelo Riquert (Coord.), (Buenos Aires: Hammurabi, 2014), 171-196.

por organizaciones virtuales transnacionales[45]. Hay que recordar que esta clase de criminalidad utiliza sitios temporales con seguridad reforzada en la deep web o de mecanismos de ocultamiento, pseudonimización para ocultar la identidad digital de los criminales, o de otras técnicas que permiten asegurar transacciones sin trazo u ocultas en monedas digitales o medios de pago digitales con equivalencia económica.

En la medida en que son delitos difíciles de rastrear o detectar, es necesario construir verdaderas políticas criminales de naturaleza preventiva, coordinadas entre los países de la región[46]. Todo ello, complementado por políticas públicas eficaces que permitan reducir la impunidad en estos crímenes.

Sin embargo, ello no podrá ser una realidad si los Estados no desarrollan e implantan mecanismos de cooperación recíproca a escala regional[47] que integren y complementen las legislaciones nacionales (COIP, arts. 488, 491, 494 y 496) para hacer posibles, entre otras actividades de cooperación ágiles, remitir rápidamente elementos y evidencias digitales a otros Estados, realizar actos de asistencia administrativa y judicial, adoptar instrumentos de extradición activa y pasiva menos burocráticos (pero igualmente respetuosos de las garantías ciudadanas) e incluso, adoptar medidas cautelares sobre datos o información requerida por otros Estados o practicar pruebas en formato electrónico por delegación.

La idea central de esta clase de mecanismos es que los jueces penales nacionales puedan desarrollar en tiempo razonable los procedimientos judiciales sobre los cibercrímenes, sin que ello sea entorpecido por oficinas de trámites internacionales en los entes de investigación o en los respectivos ministerios de relaciones exteriores. Es más, el paso a seguir es considerar que los jueces puedan ser facultados para solicitar directamente la información, a otros jueces extranjeros que sirvan de enlace judicial en el país requerido. Naturalmente, cuando ello sea previsto en acuerdos o convenios de carácter internacional.

3. Conclusión

Sin lugar a duda, los cibercrímenes y los delitos informáticos en sentido amplio constituyen un nuevo y peligroso paradigma de criminalidad que debemos combatir con todas las herramientas que brinda el modelo de Estado social y democrático de derecho. Una nueva criminalidad que no solo ha mostrado la existencia de nuevos riesgos sociales, sino que, en el ámbito jurídico, viene transformando la teoría del delito, el ejercicio profesional, e invita a replantear la mayoría de las estructuras fundamentales de la investigación y el proceso penal moderno. Es claro que esta clase de delitos no pueden ser acreditados o demostrados utilizando técnicas ordinarias de investigación en la obtención, recolección, embalaje, etc. de los elementos materiales probatorios y evidencia relevante que ahora, en su mayoría,

45 Lillian, Ablon / Martin C. Libicki/ Andrea A. Golay Markets for Cyber Crime, tools and stolen data. Hacker's Bazaar, (California: Rand, 2014), 3 y ss.

46 Kamini, Dashora. "Cyber Crime in the Society: Problems and Preventions", En: Journal of Alternative Perspectives in the Social Sciences, Feb2011, Vol. 3 Issue 1, (2011): 240-259; Óscar, Morales García. "Apuntes de política criminal en el contexto tecnológico. Una aproximación a la convención del Consejo de Europa sobre Cybercrimen", En: Delincuencia informática. Problemas de responsabilidad, Óscar Morales García (Dir.), Cuadernos de derecho judicial IX-2002 (Madrid, Consejo General del Poder Judicial, 2002), 11-34; Brittson Reyes; Steele, O'Shea. Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors, 262 y ss.

47 La Convención sobre el Cibercrimen, Budapest 23 de Noviembre de 2001, artículos 23 y ss. En general, v. Santiago Deluca y Enrique Del Carril, "Cooperación internacional en materia penal en el MERCOSUR: el cibercrimen", En: Revista De La Secretaría Del Tribunal Permanente De Revisión, (Números), (2017): 13-28. https://doi.org/10.16890/rstpr.a5.n10.p13; Kiefer Dupuy, Cibercrimen, "Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet".

es de naturaleza informática o digital.

De igual manera, la existencia de esta clase de crímenes señala la importancia real de proteger la información, los datos y los sistemas informáticos en una sociedad altamente mediática, hiperconectada a la internet y dependiente de dispositivos electrónicos e informáticos en casi todas las actividades personales y sociales. Protección que se viene ajustando de forma progresiva, pero lenta, particularmente en América Latina.

Además, las carencias del sistema penal, como se ha señalado en este texto, son múltiples, variadas y complejas; a tal punto que resulta imprescindible corregirlas rápidamente, con el fin de reducir las altas tasas de impunidad que existen en perjuicio de las víctimas y evitar mayores perjuicios económicos en nuestras sociedades. Son particularmente llamativas, aquellas deficiencias que tienen relación con aspectos sustantivos, como por ejemplo, el concepto de cibercrimen y sus diferencias con los delitos informáticos en sentido amplio, con los procedimientos judiciales para perseguirlos o judicializarlos, y con las técnicas de investigación digital o informática para demostrar su ocurrencia y descubrir a los verdaderos responsables.

Dicho lo anterior, los esfuerzos por perfeccionar la investigación y la persecución de los cibercrímenes deben orientarse a proteger las funciones informáticas (confidencialidad, integridad, disponibilidad, no repudio y capacidad de búsqueda de los datos informáticos) y la seguridad de la información de las personas, las empresas y el Estado. Pero ello debe estar precedido por la adopción de políticas públicas que refuercen la seguridad de digital, eduquen seriamente a la población en el gobierno de sus datos personales y en la protección de los datos empresariales y las estructuras críticas de la región.

4. Referencias

Aboso, Gustavo Eduardo y Zapata. María Florencia. Cibercriminalidad y derecho penal: la información y los sistemas informáticos como nuevo paradigma. Montevideo-Buenos Aires, B de F, 2006.

Ablon, Lillian, Libicki, Martin C. y Golay, Andrea A. Markets for Cyber Crime, tools and stolen data. Hacker's Bazaar. California: Rand, 2014.

Anarte Borrallo, Enrique. "Incidencias de las nuevas tecnologías en el sistema penal. Aproximación al derecho penal en la sociedad de la información". En: Derecho y conocimiento 1. (2010).

Balance Cibercrimen. (2020). Caivirtual Policia. Recuperado el marzo de 2020, de Centro cibernético policial de Colombia: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

Ballesteros, M. C. R., & Hernández, J. A. G. "Cibercrimen: Particularidades en su investigación y enjuiciamiento/Cybercrime: Particularities in investigation and prosecution". En: Anuario Jurídico y Económico Escurialense. (47). 2014.

Bautista García, Fredy; Mosquera Suárez, Álvaro José; Meneses Obando, Andrés; y Ríos Sarmiento, Daniel. Evidencia Digital. Aspectos generales. Rama Judicial, Consejo Superior de la Judicatura, Escuela Judicial Rodrigo Lara Bonilla. Bogotá, 2020.

Bednar, Peter M.; Katos, Vasilios; Hennell, Cheryl. "On the Complexity of Collaborative Cyber Crime Investigations". En: Digital Evidence and Electronic Signature Law Review. Vol. 6.

Borghello, Cristian/Temperini, Marcelo G. I. "Suplantación de identidad digital como delito informático". En: Cibercrimen, Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet, de Dupuy, Daniela (Dir.)/Kiefer, Mariana (Coord.). Buenos Aires-Montevideo: BdeF, 2017.

Cano Martínez, Jeimy. Computación forense: descubriendo los rastros informáticos. 2ª ed. Bogotá: Alfaomega, 2015.

Cross, Michel. Scene of the Cybercrime, 2.ª ed. Burlington: Syngress, 2008.

Consejo Nacional de Política Económica y social (Conpes), Documento n. º 3858, 11 de abril de 2016, Bogotá. En línea: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

Convención de las Naciones Unidas contra la delincuencia organizada transnacional y sus protocolos (En adelante, Convención de Palermo). Oficina de las Naciones Unidas Contra la Droga y el Delito, Nueva York, Naciones Unidas. 2004. https://www.unodc.org/pdf/cld/TOCebook-s.pdf

Convención sobre el Cibercrimen, Budapest 23 de Noviembre de 2001, https://www.boe.es/eli/es/ai/2001/11/23/(1)/dof/spa/pdf.

Dashora, Kamini. "Cyber Crime in the Society: Problems and Preventions". En: Journal of Alternative Perspectives in the Social Sciences, Feb2011. Vol. 3 Issue 1.

Da-Yu, Kao; Ni-Chen, Wu; Fuching, Tsai. "The Governance of Digital Forensic Investigation in Law Enforcement Agencies". 21st International Conference on Advanced Communication Technology (ICACT). PyeongChang, Korea (South), 2019. 61-65. DOI: 10.23919/ICACT.2019.8701995.

De La Cuesta Arzamendi, José Luis (Dir.) /De La Mata Barranco, Norberto J. (Coord.). Derecho penal informático. Madrid: Civitas-Thomson Reuters, 2010.

Deluca, Santiago y Del Carril, Enrique. "Cooperación internacional en materia penal en el MERCOSUR: el cibercrimen". En: Revista De La Secretaría Del Tribunal Permanente De Revisión, 2017. https://doi.org/10.16890/rstpr.a5.n10.p13

Dupuy, Daniela (Dir.) y Kiefer, Mariana (Coord.). Cibercrimen, Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet. Buenos Aires-Montevideo: BdeF, 2016.

Dupuy, Daniela. Cibercrimen II: nuevas conductas penales y contravencionales, inteligencia artificial aplicada al derecho penal y procesal penal, novedosos medios probatorios para recolectar evidencia digital, cooperación internacional y victimología; prólogo Marcos Salt Buenos Aires: B de F, 2018.

Eckenwiler, M; McCulloch, S. National Security Cyber Investigations: Considerations and Challenges. United States Attorneys' Bulletin [s. l.]. v. 67. n. 1. 2019. http://search.ebscohost.com/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.usab67.8&lang=es&site=eds-live&scope=site

Galán Muñoz, Alfonso. El fraude y la estafa mediante sistemas informáticos: análisis del artículo 248.2 C.P. Valencia: Tirant lo Blanch, 2005.

Geers, Kenneth. "The Cyber Threat to National Critical Infraestructures: Beyond Theory". En: Information Security Journal: A Global Perspective. Jan2009. Vol. 18 Issue 1. 1-7. DOI: 10.1080/19393550802676097.

Gonzalez, Jason P; Esworthy, Matthew A S y Gauger, Neal J. Criminal Justice; CASES WITHOUT BORDERS: The Challenge of International Cybercrime Investigations. Chicago Tomo 30. N. º 4. 2016.

Informe Explicativo del Convenio contra el Cibercrimen, ETS-185, del Consejo de Europa y el Parlamento Europeo. https://rm.coe.int/16802fa403.

Kyung-Shick Choi, Toro-Álvarez y Marlon Mike. Cibercriminología: guía para la investigación del cibercrimen y mejores prácticas en seguridad digital= Cybercriminology: guide for cybercrime investigation and best practices in digital security. Bogotá: Universidad Antonio Nariño; Boston MA: Boston University, 2017.

Learner, De. Electronic Crime Scene Investigation. New York. Nova Science Publishers Inc; 2009. http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=311082&lang=es&site=eds-live&scope=site

Marcella, Albert J., Guillossou, Frederic. Cyber Forensics: From Data to Digital Evidence. New Jersey: Wiley, 2012.

Matellanes Rodríguez, Nuria. "Algunas notas sobre las formas de delincuencia informática en el Código penal". En: Hacia un Derecho penal sin fronteras. Coord. María Rosario Diego Díaz-Santos y Virginia Sánchez López. XII Congreso Universitario de Alumnos de Derecho penal. Madrid: Colex, 2000.

Mayer Lux, Laura. "Defining cyberterrorism". En: Revista Chilena de derecho y tecnología, vol. 7. núm. 2. 2018. DOI 10.5354/0719-2584.2018.51028.

Meek Neira, Michael. Delito informático y cadena de custodia. Bogotá: Universidad Sergio Arboleda, 2013.

Miró Llinares, Fernando. El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons, 2012.

Morales García, Óscar. "Apuntes de política criminal en el contexto tecnológico. Una aproximación a la convención del Consejo de Europa sobre Cybercrimen", En: Delincuencia informática. Problemas de responsabilidad, Óscar Morales García (Dir.), Cuadernos de derecho judicial IX-2002. Madrid. Consejo General del Poder Judicial. 2002.

Nirkhi, S. M. Dharaskar, R. V. and Thakre, V. M. "Analysis of online messages for identity tracing in cybercrime investigation," Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). Kuala Lumpur. Malaysia. 2012. DOI: 10.1109/CyberSec.2012.6246131.

Organización de Estados Americanos. Resolución AG/RES. 2026 (XXXIV-O/04) contra la Delincuencia Organizada Transnacional en el Hemisferio, aprobada en la cuarta sesión plenaria de la Organización de Estados Americanos (OEA), celebrada el 8 de junio de 2004: http://www.oas.org/juridico/spanish/ag04/agres_2026.html;

Patil, Rachana y Devane, Satish R. "Network Forensic Investigation Protocol to Identify True Origin of Cyber Crime". En: Journal of King Saud University - Computer and Information Sciences. January 2019. DOI: 10.1016/j.jksuci.2019.11.016.

Parker, Donn B. Fighting computer crime, a new framework for protecting information. EE.UU: Wiley, 1998.

Posada Maya, Ricardo. "Aproximación a la Criminalidad informática en Colombia", En: Revista de derecho, comunicaciones y nuevas tecnologías. núm. 2. Cijus-Gecti, Universidad de los Andes. Bogotá. 2006.

_____. "El Cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual". En: Revista Nuevo Foro Penal, Vol. 13 n. ˚ 13. enero-junio. Medellín. Universidad EAFIT. 2017. ISSN 0120-8179.

_____. Los cibercrímenes: Un nuevo paradigma de criminalidad. Un estudio del título VII Bis del Código Penal Colombiano. Colección Ciencias Penales. De: Ricardo Posada Maya (Dir.). Bogotá. Ed. Uniandes-Ed. Ibáñez. 2017. ISBN 978-958-749-815-8 http://dx.Doi.Org/10.15425/2017.103

_____. "¿Puede ser el cibercrimen un delito transnacional?". En: Temas de Derecho penal económico y patrimonial. Medellín. Universidad Pontificia Bolivariana, 2018. ISBN. 978-958-764-251-7.

Picotti, Lorenzo. "Internet y derecho penal: ¿un empujón únicamente tecnológico a la armonización internacional?". En: AA.VV. El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales. Carlos María Romeo Casabona (Coord.). Estudios de Derecho penal y Criminología, n. ˚ 78. Granada: Comares, 2006.

Prunckun, Henry W. "Intelligence and Private Investigation: Developing Sophis-

ticated Methods for Conducting Inquiries". Charles C Thomas. 2013. Accessed April 16. 2021. http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=608003&lang=es&site=eds-live&scope=site

Quintero Olivares, Gonzalo. "Problemas de la perseguibilidad de los ciberdelitos". En: Ciberdelitos. Grooming – Stalking – Bullying – Sexting – Ciber odio – Propiedad intelectual – Problemas de perseguibilidad –Ciberpornografía infantil, Marcelo Riquert (Coord.). Buenos Aires: Hammurabi, 2014.

Reporte de Ciberseguridad 2020 del BID y la OEA, sobre los Roesgos, avances y el camino a seguir en América Latina y el Caribe, que puede consultarse en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Reyes, Anthony; Brittson, Richard; O'Shea, Kevin; Steele, James. Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors, Rockland, MA, Syngress. 2007. http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=211407&lang=es&site=eds-live&scope=site

Rovira Del Canto, Enrique. Delincuencia informática y fraudes informáticos. Estudios de Derecho penal No. 33, (Dir.) Carlos María Romeo Casabona. Granada: Comares, 2002.

Sánchez Domingo, María Belén. "Robo de identidad personal a través de la manipulación o el acceso ilegítimo a sistemas informáticos, ¿Necesidad de una tipificación específica?", En: Revista General de Derecho Penal (IUSTEL). No. 26, noviembre de 2016, No. 418038, PDF on-line. España. 1/34.

Sankhwar, S., Pandey, D., Khan, R.A. "A Step Towards Internet Anonymity Minimization: Cybercrime Investigation Process Perspective". En Information and Decision Sciences. Advances in Intelligent Systems and Computing, Satapathy S., Tavares J., Bhateja V., Mohanty J. (eds). vol. 701. 2018. Springer. Singapore. https://doi-org.ezproxy.uniandes.edu.co:8443/10.1007/978-981-10-7563-6_27

Satzger, Helmut. "La protección de datos y sistemas informáticos en el derecho penal alemán europeo. Tentativa de una comparación con la situación legal en Colombia". En: Derecho penal y nuevas tecnologías. A propósito del título VII bis del Código Penal, Memorias 4. Fernando Velásquez Velásquez, Renato Vargas Lozano, Juan David Jaramillo Restrepo (Comp.). Bogotá: Universidad Sergio Arboleda, 2016.

Shipley, Todd G., Bowker, Art. Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace, Syngress, 2014. Accessed April 16, 2021. http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=503592&lang=es&site=eds-live&scope=site

Sieber, Ulrich. Computerkriminalität und Strafrecht. Neue Entwicklungen in Technik und Recht, 2a ed. Köln-Berlin-Bonn-München: Heymanns, 1980.

Sofaer, Abraham D., Goodman, Seymour E. "Cyber Crime and Security. The transnational dimension". En: Hoover Press. Cyber. SF. 6 y ss. En: http://media.hoover.org/sites/default/files/documents/0817999825_1.pdf

Stancu, AI. "Cybercriminals and the Victims of Cybercrime". En: Journal of Law and Administrative Sciences [s. l.]. V. 14. N. 14, p. 127–136. 2020. http://search.ebscohost.com/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.jladsc14.17&lang=es&site=eds-live&scope=site

Suárez Sánchez, Alberto. Manual de delitos informático en Colombia. Análisis dogmático de la ley 1273 de 2009. Bogotá: Universidad Externado de Colombia, 2016.

Tiedemann, Klaus. "Criminalidad mediante computadoras". En: Nuevo Foro Penal No. 30, traducido por trad. de Amelia Mantilla viuda de Sandoval. Octubre–diciembre. Bogotá: Temis, 1985.

Unión Internacional de Telecomunicaciones (UIT/ITU). Understanding Cybercrime: phenomena, challenges and legal response. Ginebra. UIT. 2012. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Velásquez Velásquez, Fernando. "Criminalidad informática y derecho penal: Una reflexión sobre los desarrollos legales colombianos". En: Derecho penal y nuevas tecnologías. A propósito del título VII bis del Código Penal, Memorias 4, Fernando Velásquez Velásquez, Renato Vargas Lozano, Juan David Jaramillo Restrepo. Bogotá: Universidad Sergio Arboleda, 2016.

Wall, David S. "Criminalizing cyberspace: the rise of the Internet as a 'crime problem'".

_____. Cybercrime. The transformation of crime in the information age, UK: Polity, 2007.

Zúñiga Rodríguez, Laura. Criminalidad organizada y sistema de derecho penal. Contribución a la determinación del injusto penal de organización criminal. Granada: Comares, 2009.

_____. "El concepto de criminalidad organizada transnacional: problemas y propuestas". En: Revista Nuevo Foro Penal Vol. 12, No. 86. enero-junio 2016. Universidad EAFIT. Medellín.

PERFIL

CRIMINOLÓGICO

LA OMISIÓN IMPROPIA EN LOS DELITOS DE APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS. TRANSFERENCIA ELECTRÓNICA DE UN ACTIVO PATRIMONIAL

Y LA RESPONSABILIDAD PENAL DE LOS ADMINISTRADORES DE LAS INSTITUCIONES DEL SISTEMA FINANCIERO

SANTIAGO ACURIO DEL PINO[1]

Para empezar es necesario definir qué es el fraude informático. La conceptualización más generalizada señala que el fraude informático es:

> **[...] el conjunto de conductas dolosas que, valiéndose de cualquier manipulación fraudulenta, modifiquen o interfieran el funcionamiento de un programa informático, sistema informático, sistema de información o alguna de sus partes componentes, para producir un perjuicio patrimonial a la víctima y la consiguiente ventaja patrimonial ilícita, a favor de su perpetrador o un tercero.**

1 Abogado en libre ejercicio. Profesor universitario.

Ahora, de acuerdo al profesor chileno Bustos Ramírez (citado por Novoa Monreal), la característica básica de la omisión es que es un concepto en referencia, es decir, la omisión está en relación a la acción[2], esta no existe por sí sola. Por tanto, detrás de una omisión hay siempre una norma de mandato[3]. Son estas normas las que dan nacimiento a los deberes y obligaciones de los ciudadanos para la convivencia en sociedad. Son esos deberes jurídicos los que dan sentido a la idea de omisión, esto ocurre en un primer momento porque al ser la omisión una conducta esperada (deber de actuación) y, por tanto, constituida siempre desde un sistema normativo o de valoraciones, sus manifestaciones exteriores siempre serán perceptibles y el núcleo de su concepto (no hacer, no obrar) se manifestará como acción negativa; y, por otro lado, la omisión como la falta de acción que se estaba obligado a realizar (deber de hacer).

De acuerdo a la Constitución de la República, las actividades financieras son un servicio de orden público[4] y podrán ejercerse previa autorización del Estado. Así, tendrán la finalidad fundamental de preservar los depósitos y atender los requerimientos de financiamiento para la consecución de los objetivos de desarrollo del país.

Para Diógenes Castellín, los servicios públicos son las actividades asumidas por órganos o entidades públicas o privadas, para dar satisfacción en forma regular y continua a cierta categoría de necesidades de interés general, bien sea en forma directa, mediante concesionario o, a través de cualquier otro medio legal, con sujeción a un régimen de derecho público o privado, según corresponda[5]. En el caso particular, las entidades financieras pertenecientes al sistema financiero privado son creadas en base al Código Monetario y satisfacen en forma regular y continua la necesidad de los ciudadanos de la intermediación y la prestación de servicios financieros[6]; actividades que son siempre de interés general y público, en el marco de la Constitución y la ley.

Por otra parte el artículo 52 de la Constitución señala que "[l]as personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa[7]". Además, la Ley Orgánica de Defensa al Consumidor determina que es derecho de los consumidores el acceso a "una información adecuada, veraz, clara, oportuna y completa sobre los bienes y servicios ofrecidos en el mercado, así como sus precios, características, calidad, condiciones de contratación y demás aspectos relevantes de los mismos, incluyendo los riesgos que pudieren prestar[8]".

En este sentido, la Carta Magna dispone que

> **[l]as personas o entidades que presten servicios públicos o que produzcan o comercialicen bienes de consumo, serán responsables civil y penalmente por la deficiente prestación del servicio, por la calidad defectuosa del producto, o cuando sus condiciones no estén de acuerdo con la publicidad efectuada o con la descripción que incorpore.[9]**

2 Los delitos de omisión se clasifican en delitos de omisión propia, omisión impropia y comisión por omisión.

3 Eduardo Novoa Monreal, "Los Delitos de Omisión", en Memorias del XII Congreso Internacional de Derecho Penal del Cairo (El Cairo: 1984), 876.

4 El concepto de orden público ha ido modificándose a lo largo del tiempo, ya que, aunque la expresión siga utilizándose como garantía de la seguridad pública, su contenido ha ido evolucionando desde la conminación de ciudadanos al cumplimiento de la norma, a la garantía de la calidad de vida de los mismos.

5 Diógenes Castellín, "Servicios Públicos", Monografías.com, 16 de enero de 2006, http://www.monografias.com/trabajos31/servicios-publicos/servicios-publicos.shtml.

6 Art. 143.- Actividad financiera. Código Monetario.- La actividad financiera es el conjunto de operaciones y servicios que se efectúan entre oferentes, demandantes y usuarios, para facilitar la circulación de dinero y realizar intermediación financiera; tienen entre sus finalidades preservar los depósitos y atender los requerimientos de financiamiento para la consecución de los objetivos de desarrollo del país. Las actividades financieras son un servicio de orden público, reguladas y controladas por el Estado, que pueden ser prestadas por las entidades que conforman el sistema financiero nacional, previa autorización de los organismos de control, en el marco de la normativa que expida la Junta de Política y Regulación Monetaria y Financiera.

7 Ecuador, Constitución de la República del Ecuador, Registro Oficial 449, 20 de octubre de 2008, art. 52.

8 Ecuador, Ley Orgánica de Defensa del Consumidor, Registro Oficial 116, Suplemento, 10 de julio de 2000, art. 4 numeral 4.

De este modo, se configuran las actividades financieras tanto como un servicio público, así como un servicio de orden público[10], considerados como el núcleo, el aspecto central más sólido y perdurable del orden social. Representan el conjunto de aquellas características y valores de la convivencia que una sociedad considera como "no negociables", es decir, aquellos elementos que determinan una relación social ordenada, segura, pacífica y equilibrada. La ruptura del orden público puede dar lugar a la imposición de una sanción dependiendo de la gravedad de la ruptura, desde una sanción civil, pasando por una administrativa, hasta una sanción penal, como señala la Constitución.

En este contexto, se debe recordar que la finalidad de las instituciones financieras, de acuerdo a la Constitución, es preservar los depósitos de los usuarios del sistema financiero. Las reglas de interpretación legal señalan que hay que tomar en cuenta la intención del constituyente y el sentido gramatical de las expresiones lingüísticas usadas en la Carta Magna. Así, la palabra usada por la Constitución es un verbo transitivo (preservar) el cual exige la presencia de un objeto directo (llamado también "complemento directo"), para tener un significado completo. Aquello hace referencia a las acciones que transitan desde el actor al objeto. En consecuencia, el actor aquí es el sistema financiero y el objeto lo constituyen los depósitos de los usuarios del sistema.

Zaffaroni señala que, al describir la conducta debida (mandato), los tipos omisivos propios de *prima facie* no definen acciones. En este caso, la obligación de los bancos, en relación a su deber de custodia, es tutelar, salvaguardar, proteger y preservar el patrimonio que les ha sido encomendado para cuidarlo. Todo ello asociado a una incuestionable vocación de servicio al cliente.

Muñoz Conde afirma que la omisión social y jurídicamente reconocida está referida siempre a una acción determinada, cuya no realización constituye su esencia[11]. Es así que el sujeto activo autor de la omisión debe estar en condiciones de poder realizar la acción. Por tanto, la omisión no es un simple "hacer nada", sino no realizar una acción que el sujeto está en situación de poder hacer y que se espera que haga. En conclusión, las conductas omisivas solamente sancionan la no realización de la conducta que es debida y que se pudo realizar y hacer, por cuanto es esperada por el ordenamiento jurídico positivo[12].

En el caso de la omisión de las instituciones bancarias, se presupone siempre la existencia de un determinado sistema de relaciones sociales del cual surge la exigencia de que los funcionarios y administradores del sistema financiero, en determinadas condiciones (mismas que estarán señaladas en el ordenamiento jurídico: principio de legalidad), lleven a cabo una determinada acción. Esta acción consiste en custodiar con responsabilidad los valores depositados en cada una de las instituciones financieras. Depósitos generados por la confianza que los ciudadanos tienen en el servicio que el sistema presta, y que se ve defraudado por la laxitud de los controles, la falta de información, capacitación y la carencia de medidas preventivas eficaces y personalizadas que eviten esta clase de comportamiento disvaliosos.

9 Ecuador, Constitución de la República del Ecuador, art. 54.

10 El derecho de los consumidores va dirigido al orden público que ha ido evolucionando hasta comprender aspectos de carácter económico y social. Dentro de este "orden público económico", se distingue el llamado orden público de dirección, en virtud del cual el Estado fija determinados objetivos económicos, resultando necesario, en algunos supuestos, que ciertos actos privados sean autorizados por aquel. En este caso en particular, se encuentran las instituciones financieras públicas y privadas. Por otro lado existe el orden público de protección, que persigue resguardar y tutelar a una de las partes con el objetivo de proteger el equilibrio interno del contrato de servicios financieros y bancarios. Paula Castro, Raúl Farías y Nora Cherñavsky, "Derecho de los Consumidores", Novedades Jurídicas, n.° 62 (2011): 32-45.

11 Francisco Muñoz Conde, Teoría General del Delito (Bogotá: Editorial NOMOS, 1999), 23.

12 Desde su razonamiento, este autor solo acepta la omisión propia, más no la impropia por estar reñida con el principio de legalidad. Eugenio Raúl Zaffaroni, Manual de Derecho Penal (Buenos Aires: Editorial EDIAR, 2007), 317.

El artículo 23 del Código Orgánico Integral Penal menciona:

> **Art. 23.- Modalidades de la conducta.- La conducta punible puede tener como modalidades la acción y la omisión. No impedir un acontecimiento, cuando se tiene la obligación jurídica de impedirlo, equivale a ocasionarlo[13].**

De este modo, se puede afirmar que, desde la perspectiva constitucional, legal y hasta contractual, los bancos tienen el deber de protección y custodia sobre los depósitos de sus clientes, así como el de informarlos y capacitarlos sobre el uso de canales electrónicos y banca en línea. Por tanto, la omisión adquiere relevancia por concretar el incumplimiento de dichas obligaciones jurídicas con miras a evitar la realización de un acto de disposición patrimonial perjudicial, siempre y cuando –como en el caso de las instituciones financieras– quienes omiten estos deberes tengan la obligación de actuar según el ordenamiento jurídico positivo.

No obstante, la pregunta que surge es si esta omisión, desde el punto de vista penal, es una omisión punible o no lo es. En otras palabras, cuando los delincuentes informáticos, realizan las distintas manipulaciones informáticas que crean el peligro para el patrimonio ajeno, y este riesgo, a pesar de haberlo advertido (previsión del riesgo), no es evitado por quien ha asumido de manera voluntaria funciones de protección del bien jurídico patrimonial (derivados del ordenamiento jurídico y del contrato bancario que le imponen deberes de lealtad o fidelidad), es posible determinar que ese garante[14] (institución bancaria, sus administradores y personal operativo) es el responsable del delito de fraude informático por omisión (comisión por omisión).

Como se había mencionado, la no evitación del resultado equivale a su producción. Así, desde la dogmática penal, la respuesta es que sí. Además, en los delitos de apropiación fraudulenta por medios electrónicos y transferencia electrónica de activo patrimonial se encuentran delitos de omisión impropia. Aquello tomando en consideración los siguientes elementos:

ELEMENTOS	DESCRIPCIÓN
Delitos de omisión impropia o de comisión por omisión	Apropiación fraudulenta por medios electrónicos y la transferencia electrónica de un activo patrimonial.
Descripción típica	**Art. 190.-** La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. **Art. 231.-** La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años[15].
Clase de norma	Son normas de prohibición en lo básico, pero hay obligaciones de segundo grado de actuar, en este caso el deber de informar el uso correcto del sistema de información y redes electrónicas relacionadas con los canales electrónicos y la banca en línea por parte de las instituciones financieras a sus clientes y usuarios y de proteger su patrimonio.

13 Ecuador, Código Orgánico Integral Penal, Registro Oficial 180, Suplemento, 10 de febrero de 2014, art. 23.

14 Según Muñoz Conde, el sujeto tiene la obligación de tratar de impedir el resultado en virtud de determinados deberes, cuyo cumplimiento ha asumido o le incumben en razón de su cargo o profesión. Esta obligación especial, convierte al sujeto en garante. Muñoz Conde, Teoría General del Delito, 27.

15 Ecuador, Código Orgánico Integral Penal, art. 190 y 231.

Contenido del imperativo	Impedir el perjuicio patrimonial lesivo a los clientes de las instituciones financieras producido por este delito en todas sus modalidades.
Finalidad social	Hacer efectiva la obligación constitucional que tienen las instituciones financieras de preservar el dinero de los usuarios del sistema (art. 308 de la Constitución). Como garantía para la protección del derecho a la propiedad y el derecho de los consumidores y usuarios a recibir bienes y servicios de calidad. (art. 52, y 66 numeral 26 de la Constitución)
Sujeto activo posible	Solo el que está en posición de garante que tenga dominio del hecho fundamento o causa del resultado, además tenga una función protectora del bien jurídico protegido es decir una especial vinculación por mandato constitucional, legal y contractual.

Por otro lado, los Artículos 152 y 157 del Código Monetario señalan:

> **Art. 152.-** Derechos de las personas. Las personas naturales y jurídicas tienen derecho a disponer de servicios financieros de adecuada calidad, así como a una información precisa y no engañosa sobre su contenido y características [...]
>
> **Art. 157.-** Vulneración de derechos. Los usuarios financieros podrán interponer quejas o reclamos ante la propia entidad, organismo de control o al Defensor del Cliente o plantear cualquier acción administrativa, judicial o constitucional reconocida en la ley para exigir la restitución de sus derechos vulnerados y la debida compensación por los daños y perjuicios ocasionados.

En ese sentido y, en concordancia con el Reglamento a la Ley de Comercio Electrónico[16], la prestación de servicios electrónicos que impliquen el envío por parte del usuario de información personal, confidencial o privada, requerirá el empleo de sistemas seguros en todas las etapas del proceso de prestación de dicho servicio.

Además, es obligación de quien presta los servicios en línea de intermediación financiera y bancaria, el informar en detalle a los usuarios sobre el tipo de seguridad que utiliza, sus alcances y limitaciones, así como sobre los requisitos de seguridad exigidos legalmente y si el sistema puesto a disposición del usuario cumple con los mismos. En caso de no contar con seguridades, se deberá informar a los usuarios de este hecho en forma clara y anticipada previo el acceso a los sistemas o a la información, e instruir claramente sobre los posibles riesgos en que puede incurrir por la falta de dichas seguridades.

Así, el Código Monetario reconoce a los usuarios del sistema financiero el derecho a recibir un servicio bancario y financiero de calidad. En consecuencia, podrían en virtud del artículo 157 del mencionado código, podrían interponer quejas o reclamos ante la propia entidad, organismo de control o al defensor del cliente[17], o plantear cualquier acción administrativa, judicial o constitucional reconocida en la ley para exigir la restitución de sus derechos vulnerados y la debida compensación por los daños y perjuicios ocasionados.

El Art. 246 del Código Monetario señala la información que debe tener el usuario financiero. De este modo, las entidades del sistema financiero nacional tienen la obligación de informar a los usuarios financieros, al menos lo siguiente:

16 Art. 21.- De la seguridad en la prestación de servicios electrónicos. - Reglamento a la Ley de Comercio Electrónico.

17 Defensor del cliente. Cada entidad integrante del sistema financiero nacional tendrá un defensor del cliente, que será independiente de la institución y designado de acuerdo con la regulación que expida la Junta. El defensor del cliente no podrá tener ningún tipo de vinculación con los accionistas o con los administradores de la entidad financiera. Su función será proteger los derechos e intereses de los usuarios financieros y estarán reguladas por la Junta de Política y Regulación Monetaria y Financiera.
Ecuador, Código Orgánico Monetario y Financiero, Registro Oficial 332, Segundo Suplemento, 12 de septiembre de 2014, art. 158.

1. Sus principales indicadores financieros;
2. Las tasas de interés activas y pasivas efectivas anuales;
3. Los cargos por servicios financieros;
4. Las condiciones generales de las actividades financieras que prestan;
5. La calificación de riesgo, cuando corresponda;
6. El estado de las operaciones que un usuario mantenga con la entidad;
7. Los beneficios y limitaciones de los servicios que se están ofertando;
8. El procedimiento para la atención de los reclamos ante la institución financiera;
9. Un ejemplar del documento físico, cuando la institución financiera requiera la firma del usuario: y,
10. En caso de acordar que ciertos servicios, como los estados de cuenta, sean enviados de manera electrónica, la certificación bancaria física que se requiera no tendrá costo.

Por otro lado, en el artículo 255 del Código Monetario se encuentran las prohibiciones a entidades del sistema financiero nacional. Se incluye la prohibición a dichas entidades, de realizar cualquier forma de publicidad engañosa, abusiva o que induzca a error en la elección de los servicios, que pueda afectar los intereses y derechos de los usuarios financieros.

Estos dos artículos del Código Monetario refuerzan la idea de que las instituciones del sistema financiero nacional deben brindar toda la información a los usuarios sobre el uso de la banca en línea y también sobre la seguridad de las tarjetas de débito y crédito.

Alberto Suárez Sánchez, en su obra denominada La estafa informática, señala claramente que los sujetos activos (administradores de las instituciones del sistema financiero y sus funcionarios) obligados a evitar la producción del resultado nocivo no cumplieron

> **[...] con su posición de garante y además hay una equivalencia valorativa entre la omisión realizada y la conducta típica de los delitos analizados (apropiación fraudulenta por medios electrónicos y transferencia de un activo patrimonial). A pesar de que los sujetos no crearon el riesgo de producción de una transferencia de activos perjudicial para el bien jurídico si lo incrementaron, pues no hay duda que si hubieran realizado la acción debida (protección de los depósitos) el resultado nocivo no se hubiere ocasionado. El contenido del injusto de quien no realizó la acción para evitar la producción del resultado lesivo para el patrimonio es equivalente a de quien la realiza la manipulación informática que determina la transferencia patrimonial que a su turno causa perjuicio, es decir aquel tiene la misma relevancia que este porque se presenta como causa determinante de la producción del resultado típico.[18]**

Así, la responsabilidad por la comisión por omisión de los delitos de apropiación fraudulenta por medios electrónicos y transferencia electrónica de activo patrimonial (fraudes informáticos) se debe principalmente a la falta de cumplimiento de la función de garante que les otorga la Constitución, la ley y el contrato a los administradores de las instituciones del sistema financiero

18 Alberto Suárez Sánchez, La Estafa Informática (Bogotá: Grupo Editorial Ibáñez: 2009).

y los funcionarios subyacentes. Paralelamente, se debe considerar que ellos tienen el dominio del hecho fundamento del resultado, al ser una obligación implementar las políticas y directrices referentes a la prestación de los servicios financieros.

Ciertamente, son parte de las políticas de prestación de servicios financieros elementos como la educación al usuario financiero, el control interno, la evaluación de los riesgos del negocio y, sobre todo, de la banca en línea[19]. Por tal razón, si los administradores de las instituciones financieras fallan en definir y controlar la ejecución de estas políticas y directrices, así como de las obligaciones dispuestas en el artículo 4 de la Ley de Defensa al Consumidor relativas a la información que deben brindar al consumidor (en concordancia con el artículo. 53 y 54 de la Constitución, artículos. 152, 246 y 255.16 del Código Monetario y el Art. 21 del Reglamento a la Ley de Comercio Electrónico), esta omisión puede establecerse como el fundamento del resultado; entendido este como el perjuicio patrimonial sufrido por los clientes de las instituciones financieras del país al ser víctimas de estos delitos.

El posible problema surge, por un lado, por el principio de legalidad, ya que al ser esta una omisión impropia según los principios de *nulla poena sine lege scripta y nulla poena sine lege stricta*, podría decirse que este tipo va en contra de lo dispuesto en el Art. 5.1 del Código Orgánico Integral Penal, el cual está en concordancia con el artículo 76 numeral 3 de la Constitución y, por ello, sería posiblemente inconstitucional. No obstante, desde un criterio personal, alineado a lo señalado por Schünemann[20], se considera que no existe tal inconstitucionalidad, puesto que, al ser delitos de resultado, la versión comisiva de los mismos se cumple descriptivamente con la acción, mientras que la omisión se cumple de forma normativa por parte del garante, situación que no se encuentra indicada en detalle por los tipos penales de apropiación fraudulenta por medios electrónicos y transferencia electrónica de activo patrimonial (este es uno de los elementos señalados por Novoa Morreal para la existencia de esta clase de delitos de omisión impropia). De esta manera se cumple formalmente el principio de legalidad.

En definitiva, sería posible, desde la dogmática penal, el enjuiciamiento de los administradores y encargados de la seguridad de la información de los servicios financieros y bancarios de las instituciones del sistema financiero por el delito de omisión impropia, contenido en los tipos penales de apropiación fraudulenta por medios electrónicos y transferencia electrónica del activo patrimonial por parte de los perjudicados por el llamado fraude informático.

Finalmente, se debe recordar que el artículo 249[21] del Código Monetario señala que las

19 La educación financiera resulta fundamental y se hace cada vez más importante para que los usuarios del sistema financiero hagan buen uso de este, lo que contribuye a su ampliación y estabilidad. Los productos y servicios ofrecidos por las instituciones de intermediación financiera, a menudo contienen elementos que no siempre son de fácil comprensión para los usuarios. De ahí, la importancia de la instrucción que se otorgue a estos, para lograr que la bancarización genere resultados positivos, manteniendo la estabilidad y competitividad del sistema. La base esencial de tal derecho es su consideración como presupuesto fundamental para el desarrollo de la libre elección de los consumidores. Al igual que ocurre con el derecho a la información, solo cuando los usuarios están debidamente informados y capacitados pueden tomar decisiones acordes con sus necesidades e intereses particulares y contribuir con el avance del sistema financiero. Esto de acuerdo al informe presentado por la Federación Latinoamericana de Bancos (FELABAN).
Alejandra Quevedo, "Protección del Consumidor: Elaboración y establecimiento de mejores prácticas en la protección al usuario de servicios financieros" (informe, III Congreso Latinoamericano de Bancarización y Microfinanzas, Asunción, 30 de junio – 1 de julio de 2011), https://www.yumpu.com/es/document/read/50136510/archivo-adjunto-felaban.

20 Bernd Schünemann, Fundamento y Límites de los Delitos impropios, trad. Joaquín Cuello contreras y José Luis Serrano González de Murillo (Madrid: Editorial Marcial Pons, 2009), 91

21 Art. 249 Código Monetario.- En caso de pérdida, sustracción, robo o hurto de tarjetas de débito, crédito, de cajero automático, cheques o cualquier otro instrumento que tenga similar objetivo, las entidades del sistema financiero nacional suspenderán cualquier cargo o pago por cuenta de sus clientes, a partir de la hora en que se notifiquen dichos eventos, ya sea por escrito, por teléfono o por cualquier otro medio que constituya medio de prueba, de acuerdo con lo previsto en la ley. Los cargos o pagos efectuados por la entidad financiera por cuenta de sus clientes, que no hayan tomado en cuenta la notificación de pérdida, sustracción, robo o hurto, serán asumidos por la entidad. La entidad asumirá además las responsabilidades que se deriven de fraudes informáticos causados por la debilidad o defectos en sus sistemas. Los cargos o pagos efectuados por las entidades financieras por cuenta de sus clientes imputables a estos serán de su propia responsabilidad.

instituciones financieras asumirán las responsabilidades (civiles, administrativas y penales) que se deriven de los fraudes informáticos causados por la debilidad o defectos en sus sistemas. Dicha descripción podría indicar la existencia de responsabilidad penal también para la persona jurídica –una institución financiera– a la luz de los artículos 49 y 71 del Código Orgánico Integral Penal. Aquello, puesto que, al no reconocer los perjuicios por la omisión de quienes ejercen el control de sus órganos administrativos, y quienes cumplan actividades de administración, dirección y supervisión la institución financiera, la persona jurídica se beneficia del dinero público de sus clientes. Esto ahora queda refrendado por la reforma publicada en el Registro Oficial, Cuarto Suplemento No. 526 del 30 de Agosto del 2021, en donde se incluye el artículo 234.3[22] señalando claramente que los delitos contra la seguridad de los activos de los sistemas de información y comunicación (entre los que está incluido el artículo 231 antes comentado), generan responsabilidad penal para las personas jurídicas, en este caso, para las instituciones del sistema financiero.

22 Ley Orgánica reformatoria del Código Orgánico Integral Penal, para prevenir y combatir la violencia sexual digital y fortalecer la lucha contra los delitos informáticos. "Art. 234. 3.- Responsabilidad de personas jurídicas.- A los delitos de esta Sección es aplicable la responsabilidad prevista en los artículos 49 y 71 de este Código".

Bibliografía

Castellín, Diógenes. "Servicios Públicos". Monografías.com, 16 de enero de 2006. http://www.monografias.com/trabajos31/servicios-publicos/servicios-publicos.shtml.

Castro, Paula, Farías, Raúl y Cherñavsky, Nora. "Derecho de los Consumidores", Novedades Jurídicas, n.° 62 (2011).

Ecuador. Código Orgánico Integral Penal. Registro Oficial 180, Suplemento, 10 de febrero de 2014.

Ecuador. Código Orgánico Monetario y Financiero. Registro Oficial 332, Segundo Suplemento, 12 de septiembre de 2014.

Ecuador. Constitución de la República del Ecuador. Registro Oficial 449, 20 de octubre de 2008.

Ecuador. Ley Orgánica de Defensa del Consumidor. Registro Oficial 116, Suplemento, 10 de julio de 2000.

Ecuador. Ley orgánica reformatoria del código orgánico integral penal, para prevenir y combatir la violencia sexual digital y fortalecer la lucha contra los delitos informáticos. Registro Oficial 526, Cuarto Suplemento, 10 de julio de 2000.

Ecuador. Reglamento general a la ley de comercio electrónico, firmas electrónicas y mensajes de datos. Registro Oficial 735, 30 de agosto de 2021.

Muñoz Conde, Francisco. Teoría General del Delito. Bogotá: Editorial NOMOS, 1999.

Novoa Monreal, Eduardo. "Los Delitos de Omisión". En Memorias del XII Congreso Internacional de Derecho Penal del Cairo. El Cairo: 1984.

Schünemann, Bernd. Fundamento y Límites de los Delitos impropios. Traducido por Joaquín Cuello contreras y José Luis Serrano González de Murillo. Madrid: Editorial Marcial Pons, 2009.

Suárez Sánchez, Alberto. La Estafa Informática. Bogotá: Grupo Editorial Ibáñez: 2009.

Quevedo, Alejandra. "Protección del Consumidor: Elaboración y establecimiento de mejores prácticas en la protección al usuario de servicios financieros". Informe presentado en el III Congreso Latinoamericano de Bancarización y Microfinanzas, Asunción, 30 de junio – 1 de julio de 2011.https://www.yumpu.com/es/document/read/50136510/archivo-adjunto-felaban.

Zaffaroni, Eugenio Raúl. Manual de Derecho Penal. Buenos Aires: Editorial EDIAR, 2007.

PERFIL CRIMINOLÓGICO

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD EN EL ECUADOR

GABRIEL LLUMIQUINGA VEINTIMILLA[1]

Desde hace un poco más de 20 años el Ecuador empezó a experimentar el impacto del uso de las tecnologías de la información y comunicación (TIC) en el sector público y privado. Uno de los primeros servicios en línea, allá por el año 2000, fue el de una institución financiera que implementó un portal de servicios, a través del cual, los clientes consultaban y realizaban sus trámites. En aquel entonces, los clientes de esta institución veían con mucho escepticismo y desconfianza este tipo de servicios, sin embargo, a medida que el tiempo transcurrió, su uso se volvió más frecuente, y se dio inicio a la digitalización y automatización de algunos servicios que, hasta aquel entonces, se hacían de manera manual y presencial en las agencias de atención al cliente.

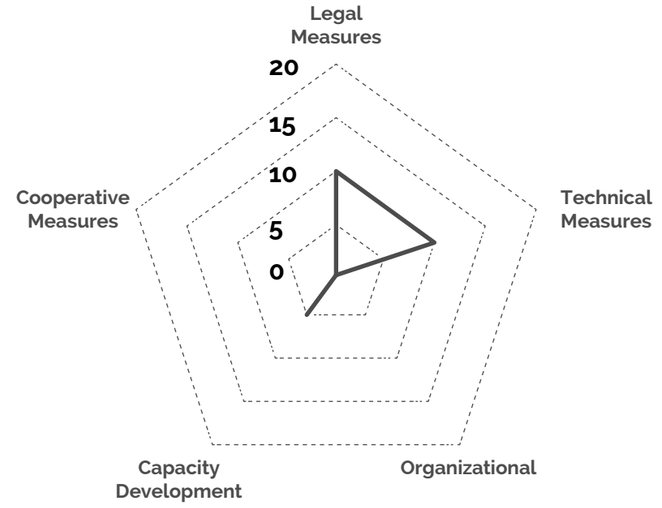
---

1 Ingeniero en Sistemas de la Universidad Politécnica Salesiana. Magister en Evaluación y Auditoría de Sistemas Informáticos por la Universidad de las Fuerzas Armadas Espe. Cuenta con un diplomado en "Cyber Crime Investigation" cursado en la Universidad de la Policía Nacional de Corea en Corea del Sur. Tiene 13 años de experiencia en los campos de auditoría, seguridad de la información, ciberseguridad, continuidad de negocio y gestión de tecnologías de la información y comunicación. Se desempeñó como especialista, coordinador y jefe de seguridad informática en varias organizaciones públicas y privadas, fue supervisor de auditoría de TI en la Contraloría General del Estado, actualmente desempeña como gerente de auditoría, riesgos y servicios en AUDETIC para Chile y Ecuador. Lidera y ejecuta proyectos importantes en instituciones públicas y privadas de la Región. Ha obtenido varios logros a través de su vida profesional, destacando las becas obtenidas para cursar la especialización en investigación de cibercrimen en Corea del Sur y participar en seminarios y cursos de ciberseguridad a nivel internacional. Cuenta con varias certificaciones internacionales que avalan su experiencia. Además, colabora activamente en la academia como docente de pregrado y posgrado de varias instituciones de educación superior. Es promotor, fundador y presidente de la Asociación Ecuatoriana de Ciberseguridad (AECI).

Desde aquel entonces, a la actualidad, la tecnología dejó de ser un elemento accesorio para convertirse en una necesidad en las interrelaciones personales y comerciales de los individuos, teniendo como principales protagonistas al internet, redes sociales y aplicaciones de mensajería instantánea.

En este contexto, la seguridad de los datos personales, la integridad de las aplicaciones, la disponibilidad de las plataformas y la seguridad de la información tomaron mayor relevancia. En la actualidad, escuchar o leer que una entidad u organización sufrió un ataque informático es muy común. Sin embargo, no es muy común conocer cómo solventaron o mitigaron aquellas amenazas que se materializaron. Asimismo, escuchar a familiares o amigos que fueron timados o estafados a través de medios electrónicos también es muy común, no obstante, tampoco es común escuchar si se realizó una denuncia y mucho menos si las entidades involucradas en el fraude, respondieron por este tipo de estafas.

Tomando como referencia los dos últimos estudios del estado de la ciberseguridad realizado por la Unión Internacional de las Telecomunicaciones (ITU), en el Ecuador se puede confirmar que el nivel de madurez de la ciberseguridad aún se encuentra en etapas iniciales. Es más, al 2020 la postura de ciberseguridad que tenía el país es menor a la que se tenía en el 2018. Para la ITU, existen áreas en las que prácticamente no se demuestra desarrollo, ni avance en materia de ciberseguridad, tal como lo muestra la **Figura 1.**



Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures

Area(s) of Relative Strength
Organizational Measures,
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
26.30	10.22	9.55	0.00	6.53	0.00

Figura 1. Estado de la ciberseguridad en el Ecuador
Fuente: ITU Global Cybersecurity Index v4 - 2021

El estudio de la ITU evidencia que, pese a los esfuerzos que ciertos actores del sector público, empresa privada, academia y sociedad civil, realizan para fortalecer la ciberseguridad a nivel nacional, estos aún no tienen el impacto estratégico y necesario que el Ecuador demanda.

Al realizar un análisis de las estrategias de ciberseguridad que se desarrollaron e implementaron en la región, se puede observar que varias fueron desarrolladas y construidas con el apoyo de la Organización de Estados Americanos (OEA), lo cual sin duda constituye un aporte significativo. Las estrategias fueron construidas teniendo como referencia el "Modelo de madurez de la capacidad de ciberseguridad para las naciones (CMM)", un marco metodológico diseñado por la Universidad de Oxford que comprende las siguientes cinco dimensiones:

1. Desarrollar políticas y estrategias de ciberseguridad;
2. Fomentar una cultura de ciberseguridad responsable en la sociedad;
3. Desarrollar conocimientos y capacidades en ciberseguridad;
4. Crear marcos legales y regulatorios efectivos; y
5. Controlar los riesgos a través de estándares y tecnologías.

Sin embargo, comparando las estrategias de ciberseguridad implementadas en la región con aquellas desarrolladas y definidas en Europa y Asia, llama la atención que, en países como Singapur, estas estrategias se establecieron sobre la base de su contexto como nación y necesidades particulares. Es decir, no se adaptó ni adoptó un modelo en particular, lo cual, tiene mucho sentido, pues, pese a que ciertos países pueden tener contextos muy similares, existen aspectos específicos que definen y caracterizan a cada uno.

Las situaciones antes descritas deben generar un debate y reflexión en los encargados de desarrollar políticas y estrategias de ciberseguridad. Si bien, el intercambio de experiencias internacionales es vital, también es importante identificar las iniciativas desarrolladas en el Ecuador, orquestarlas y construir una estrategia que no solo se enfoque en el ámbito público.

Por ejemplo, si se analiza la "Estrategia de Ciberseguridad" de Singapur, se puede identificar que esta se encuentra construida sobre tres pilares:

1. Construcción de una infraestructura resiliente, que implica:

- Fortalecer la seguridad y la resiliencia de la infraestructura digital.
- Explorar la expansión de regulación y leyes de ciberseguridad para incluir entidades y sistemas más allá de "Infraestructuras Críticas de Información". El objetivo es no tener un enfoque puramente regulatorio sino un entorno de rápida evolución.
- Adoptar una mentalidad de gestión de riesgos en todos los actores de la nación (Estado, empresa y academia). Procurando que las empresas y organizaciones inviertan en ciberseguridad.

2. Habilitar un ciberespacio más seguro, que incluye:

- Crear un entorno digital más limpio y saludable.
- Tomar desde el Gobierno la iniciativa para asegurar la infraestructura digital que impulsa la economía digital y que respalde el desarrollo de un entorno digital saludable.
- Motivar a que empresas, organizaciones y personas sean también los responsables de asegurar su entorno digital.

3. Mejorar la cooperación internacional, que comprende:

- Fomentar un ciberespacio abierto, seguro, estable, accesible, pacífico e interoperable.
- Promover el desarrollo y la implementación de normas voluntarias y no vinculantes, alineadas al derecho internacional.
- Desarrollo y adopción de estándares técnicos e interoperables.
- Intensificar la cooperación con socios internacionales para combatir las ciber amenazas transfronterizas.

Los pilares antes mencionados y que forman parte de la "Estrategia de Ciberseguridad" de Singapur se sustentan y son viables de conseguir gracias a dos "habilitadores fundamentales", estos son:

1. Desarrollar un ecosistema de ciberseguridad dinámico

Consiste en construir un ecosistema de ciberseguridad respaldado por la investigación y la innovación para las necesidades económicas y de seguridad de Singapur, para lo cual su Gobierno se compromete a impulsar la industria y el mundo académico de la ciberseguridad con la finalidad de desarrollar capacidades avanzadas, crear productos y servicios de clase mundial y hacer crecer el mercado de ciberseguridad. El Gobierno prácticamente en su estrategia se compromete a invertir en investigación e innovación en ciberseguridad, además de establecer, programas de emprendimiento, que las partes interesadas pueden aprovechar para desarrollar soluciones "Made-in-Singapore".

2. Desarrollar talentos en ciberseguridad

Consiste en desarrollar y mantener una fuerza laboral sólida en ciberseguridad que satisfaga las necesidades económicas y de seguridad de Singapur. Para lo cual, el Gobierno se compromete a trabajar en estrecha colaboración con escuelas para educar a los estudiantes y entusiastas de ciberseguridad. También, se compromete a establecer alianzas con las empresas de la industria e instituciones de educación superior que permitan desarrollar habilidades y marcos de competencias hacia trayectorias profesionales estructuradas. Y por último, el Gobierno incluye en sus estrategias alentar a personas interesadas en la ciberseguridad a que mejoren sus habilidades a través de la participación en programas de recompensas "bug bounty".

Como se puede observar, la "Estrategia de Ciberseguridad" de Singapur, básicamente enfoca sus esfuerzos en desarrollar el talento humano que permitan llevar a cabo la consecución de los tres pilares establecidos.

Por lo tanto, se podría concluir que la ciberseguridad es un aspecto estratégico en los países. Por lo tanto, debe estar gestionado al más alto nivel de Gobierno, de manera que sea aplicable a todos los sectores que componen un Estado. Delegar esta responsabilidad en una sola organización podría ocasionar que las estrategias a implementar no resulten efectivas, eficientes y se dupliquen esfuerzos y recursos.

Se debe "hacer mucho, con poco". Enfocarse en pocos objetivos (pilares) permitiría que los esfuerzos no se dispersen y que todos los involucrados trabajen de manera articulada para cumplir las metas. Además, no basta con adquirir e implementar productos tecnológicos para gestionar la ciberseguridad. Es vital invertir en el talento humano que gestiona los procesos y la tecnología en las organizaciones.

También es importante tener en cuenta que sin academia e investigación, no hay ciberseguridad. El conocimiento es fundamental. Las capacidades, competencias, destrezas y habilidades que se adquieren en las diferentes etapas educativas de los individuos deben estar enfocadas en fortalecer e implementar las estrategias de ciberseguridad de las naciones.

Si se desea obtener resultados diferentes en ciberseguridad, se deben realizar actividades que permitan obtener el efecto y resultado deseado ("pensar fuera de la caja"). Programas de recompensas (bug bounty), ejercicios cibernéticos nacionales, institucionalidad de ciberseguridad, programas académicos especializados, leyes específicas, acuerdos internacionales, incentivos para fomentar la investigación y creación de soluciones, pueden ser, entre otras actividades, las necesarias para fortalecer la ciberseguridad en el Ecuador.

PERFIL

CRIMINOLÓGICO

CIBERDELITOS: UNA PRIMERA APROXIMACIÓN Y PROYECCIÓN INSTITUCIONAL

FABIÁN CHÁVEZ[1]

I. Introducción

Los avances tecnológicos que se han venido dando en los últimos años han sido fundamentales para el crecimiento de los países y, en especial, ha provocado la reducción de la brecha digital de nuestra sociedad. Sin embargo, así como ha sido fundamental para el crecimiento y evolución tecnológica, también han revolucionado las formas de los delincuentes para realizar actividades ilícitas, configurando actos mucho más sutiles a los tradicionales que han generado daños de mucho valor a los recursos públicos o privados a nivel global.

La dependencia de la sociedad a las nuevas tecnologías de la información y de las comunicaciones (TIC), hace que resulte latente el grave daño que la delincuencia informática puede causar a la sociedad. Por ello, hoy en día, el estudio de las implicaciones sociales que representa el crecimiento de personas dedicadas a cometer delitos a través de medios tecnológicos resulta una cuestión urgente. Así, estas implicaciones asociadas al desarrollo y crecimiento de las tecnologías de la información han trascendido al ámbito del sistema jurídico actual, el cual se ha visto en la necesidad de regular las nuevas tendencias y analizar nuevos escenarios y campos de acción.

El problema surge puesto que, en la actualidad, las computadoras son utilizadas no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino que también son el medio más eficaz para la obtención de información. Hasta hace pocos años, en el Ecuador se creía tener la certeza de que nadie podía acceder a información sobre las vidas privadas, no obstante, el avance de la tecnología ha revelado que el acceso a la información personal es más fácil de lo que parece.

Así, la información sobre datos y vida personal se ha convertido en un bien muy cotizado por

1 Fiscal de la Unidad de Fuero de Corte Nacional. Fiscalía General Del Estado.

las compañías del mercado actual. La avalancha y crecimiento de las industrias computacionales y de comunicaciones ha permitido crear sistemas, que facilitan guardar grandes cantidades de información de una persona y transmitirla en muy poco tiempo. En este sentido, lo que resulta preocupante es que, más personas, empresas y organizaciones tienen acceso a esta información, sin que las legislaciones sean capaces de regularla. El mundo se encuentra frente a la era de la informática, conocida como sociedad de la información.

La informática, como un factor criminógeno, permite el acceso y manejo de bases de datos, programas de cualquier género, lesiva para los intereses de las personas y de la sociedad. Siendo muy difícil, a más de costoso, averiguar al autor del delito y la obtención de pruebas válidas dentro de un proceso penal, debido a la naturaleza de procedimiento informático. Además, si en el pasado, el delito cibernético era perpetrado principalmente por individuos o por pequeños grupos, en la actualidad se han establecido patrones bajo los cuales operan concertadamente redes delictivas muy complejas en el ciberespacio[2].

En el Ecuador, a diferencia de otras legislaciones, el ordenamiento jurídico en materia penal tiene un retraso en los últimos tiempos. Como evidencia de aquello, basta recordar que el anterior código penal era del año de 1938, generándose una brecha de 70 años hasta la reciente promulgación del Código Orgánico Integral Penal.

Con la entrada en vigencia del Código Orgánico Integral Penal, los operadores de justicia han logrado enfrentar a la llamada criminalidad informática. Con el avance de la informática y su uso en casi todas las áreas de la vida social, permite, cada vez más, el uso de la computación como medio para cometer delitos. En la mayoría de casos, esta clase de conductas quedaban en la impunidad –por ejemplo, la pornografía infantil no se encontraba regulada en el Código Penal anterior–. Por ello, de alguna manera, los tipos penales tradicionales han sido actualizados para consolidar la seguridad jurídica en el Ecuador.

Al verificarse el creciente uso indebido de los sistemas informáticos o telemáticos para la manipulación de áreas críticas, como por ejemplo, los sistemas de hospitales, aeropuertos, hidroeléctricas, telecomunicaciones, o hidrocarburos, no es difícil imaginar las incontables posibilidades que existen en cuanto a la comisión de conductas delictivas cada vez más complejas, con distintas características. Por esta razón, es necesario que la Fiscalía General del Estado, en cumplimiento de su deber constitucional y legal, instruya y facilite las herramientas necesarias a los fiscales y personal de apoyo, con el fin de combatir esta clase de ilícitos informáticos que llegan a afectar a la sociedad ecuatoriana en su conjunto.

Por otro lado, este tipo de criminalidad ha tomado mayor relevancia en el contexto actual de crisis por COVID-19. En efecto, durante este tiempo se han evidenciado los beneficios y oportunidades que brinda el uso de las tecnologías de la información y comunicación, pero también el incremento de los delitos.

II. Delitos Cibernéticos

Son varias las definiciones sobre lo que es un delito informático. La Oficina contra la Droga y el Delito de la Organización de las Naciones Unidas (UNODC) dice que "es un número ilimitado de actos contra la confidencialidad, la integridad y la disponibilidad de los datos o sistemas informáticos[3]".

2 Ecuador Ministerio de Telecomunicaciones y de la Sociedad de la Información, Política de Ciberseguridad (Quito: Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021), https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

3 Ecuador Fiscalía General del Estado, "¡Tenga cuidado!, con un solo 'clic' podría caer en la red de los delitos informáticos", Fiscalía General del Estado, 22 de noviembre de 2015, https://www.fiscalia.gob.ec/tenga-cuidado-con-un-solo-clic-podria-caer-en-la-red-de-los-delitos-informaticos/.

Por otra parte, un delito cibernético también se lo puede definir como toda actividad ilícita que:

- Se cometa mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación.

- Tenga por objeto el robo de información, robo de contraseñas, fraude financiero, pornografía infantil etc.

Desde un punto de vista jurídico, se puede definir a los delitos informáticos como toda conducta típica, antijurídica y culpable que utiliza medios tecnológicos que lesionan o ponen en peligro la libertad informática, esto es, afectando la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes y datos.

Entre los principales delitos cibernéticos se encuentran, pornografía con utilización de niñas, niños o adolescentes, apropiación fraudulenta por medios electrónicos, violación a la intimidad, acceso no consentido a un sistema informático, telemático o de telecomunicaciones, comercialización ilícita de terminales móviles, contacto con finalidad sexual con menores de dieciocho años por medios electrónicos, interceptación ilegal de datos, estafa, entre otros.

III. Evolución normativa en la legislación ecuatoriana

- En 1999 a través del proyecto de Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, el tema adquirió relevancia y discusión en el Ecuador. Al respecto, se realizaron cursos, seminarios y encuentros.

- En el 2002 aprobaron el texto definitivo de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas. En consecuencia, las reformas al Código Penal que daban luz a los llamados delitos informáticos –Expedida: Registro Oficial No. 557, 17 de Abril 2002. Estado: Vigente. Última Reforma: Suplemento del Registro Oficial 345, 8 de diciembre de 2020–.

- La ley regula mensajes de datos, firma electrónica, servicios de certificación, contratación electrónica y telemática, prestación de servicios electrónicos, a través de redes de información, comercio electrónico y la protección a los usuarios de estos sistemas.

- En el 2014 se aprobó el nuevo marco normativo penal en el país, el Código Orgánico Integral Penal (COIP) –Expedido: Registro Oficial No. 180, 10 de Febrero 2014. Estado: Vigente. Última Reforma: Registro Oficial 107, 24 de diciembre de 2019–. Antes del COIP, los delitos se encontraban en la Ley de Comercio Electrónico (referida anteriormente).

- El COIP regula los tipos penales, el procedimiento penal y el sistema penitenciario.

- Ley Orgánica Reformatoria del Código Orgánico Integral Penal en materia de anticorrupción –Registro Oficial, Segundo Suplemento No. 392. Entró en vigencia el 12 de agosto de 2021–.

De este modo, en el Ecuador, el COIP contempla y sanciona los delitos informáticos acorde a las siguientes tipificaciones

	ART.	TIPO PENAL	PENA PRIVATIVA
Pornografía Infantil	103	Pornografía con utilización de niñas, niños o adolescentes	13 a 17 años
	104	Comercialización de pornografía con utilización de niñas, niños o adolescentes	10 a 13 años
Acoso sexual "Grooming"	173	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	1 a 3 años
Ofertas de servicios sexuales a través de medios electrónicos "Sexting"	174	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	7 a 10 años
Delitos contra el derecho a la intimidad	178	Violación a la intimidad	1 a 3 años
Estafa	186	Estafa	5 a 7 años
Aprovechamiento de servicios públicos	188	Aprovechamiento ilícito de servicios públicos	6 meses a 2 años
Apropiación fraudulenta por medios electrónicos	190	Apropiación fraudulenta por medios electrónicos	1 a 3 años
Delitos referentes a terminales móviles y su información de identificación	191	Reprogramación o modificación de información de equipos terminales móviles.	1 a 3 años
	192	Intercambio, comercialización o compra de información de equipos terminales móviles	1 a 3 años
	193	Reemplazo de identificación de terminales móviles	1 a 3 años
	194	Comercialización ilícita de terminales móviles	1 a 3 años
	195	Infraestructura ilícita	1 a 3 años
Delitos contra la identidad	211	Supresión, alteración o suposición de la identidad y estado civil	1 a 3 años
Suplantación de Identidad	212	Suplantación de identidad	1 a 3 años
Revelación ilegal de información en base de datos	229	Revelación ilegal de base de datos	1 a 3 años
Interceptación ilegal de datos	230	Interceptación ilegal de datos	3 a 5 años
Fraude informático y muleros	231	Transferencia electrónica de activo patrimonial	3 a 5 años
Daños Informáticos, Malware, ataques de DoS y DDoS	232	Ataque a la integridad de sistemas informáticos	3 a 5 años
Delitos contra la información pública reservada	233	Delitos contra la información pública reservada legalmente.	5 a 7 años
Acceso no autorizado a sistemas informáticos, telemáticos o de telecomunicaciones	234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	3 a 5 años
Delitos de Terrorismo	366	Terrorismo	10 a 13 años

Fuente. Código Orgánico Integral Penal
Elaboración: Autor

IV. Estadística delitos cibernéticos

En el Ecuador, los ciberdelitos están tipificados en el Código Orgánico Integral Penal (COIP) como una medida para perseguirlos y fijar sanciones. De acuerdo con el Sistema Integrado de Actuaciones Fiscales (SIAF) de la Fiscalía General del Estado, los delitos cibernéticos que se han denunciado con mayor frecuencia a escala nacional, en los últimos 5 años son:

ART. COIP	TIPO PENAL /ARTICULO	2017	2018	2019	2020	2021[4]	TOTAL
103	Pornografía con utilización de niñas, niños o adolescentes	103	104	81	113	95	**496**
104	Comercialización de pornografía con utilización de niñas, niños o adolescentes	26	9	17	18	15	**85**
173	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	158	202	165	152	152	**829**
174	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	12	14	16	7	7	**56**
178	Violación a la intimidad	1.660	2.062	2.038	1.985	1.346	**9.091**
186	Estafa	13.911	14.268	16.918	18.415	16.272	**79.784**
188	Aprovechamiento ilícito de servicios públicos	102	130	194	99	72	**597**
190	Apropiación fraudulenta por medios electrónicos	959	1.448	1.744	2.280	3.962	**10.393**
192	Intercambio, comercialización o compra de información de equipos terminales móviles	-	-	-	1	1	**2**
193	Reemplazo de identificación de terminales móviles	4	2	-	3	-	**9**
194	Comercialización ilícita de terminales móviles	24	14	7	285	10	**340**
195	Infraestructura ilícita	-	5	7	-	-	**12**
211	Supresión, alteración o suposición de la identidad y estado civil	52	81	54	23	28	**238**
229	Revelación ilegal de base de datos	22	44	34	30	23	**153**
230	Interceptación ilegal de datos	63	41	86	73	35	**298**
231	Transferencia electrónica de activo patrimonial	54	37	50	76	170	**387**
232	Ataque a la integridad de sistemas informáticos	85	86	111	95	86	**463**
233	Delitos contra la información pública reservada legalmente.	14	12	5	5	4	**40**
234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	218	236	242	295	274	**1.265**
366	Terrorismo	12	120	65	13	17	**227**
Total general por años		**17.480**	**18.914**	**21.834**	**23.968**	**22.569**	**104.765**

Fuente: Sistema Integrado de Actuaciones Fiscales (SIAF)
Elaboración: Autor

4 Con corte al 31 de agosto

V. Cooperación interinstitucional

La Fiscalía General del Estado es el órgano de dirección, coordinación y control del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses, en materia de investigación preprocesal y procesal penal[5].

A más de las atribuciones constantes en la Constitución y en el Código Orgánico Integral Penal, deberá controlar el cumplimiento de los procedimientos estandarizados, reglamentos, manuales, protocolos técnicos, científicos y demás normativa por parte de las entidades operativas en relación a la investigación, medicina legal y ciencias forenses.

- Así, la Fiscalía ejerce sus atribuciones con cobertura nacional en beneficio de todos los habitantes. En particular, el trabajo de investigación en delitos cibernéticos lo realiza de manera estrecha con diferentes unidades investigativas como:

- Dirección Nacional de Ciberdelitos de la Policía Nacional

- Sección de informática forense de Criminalística del Servicio Nacional De Medicina Legal y Ciencias Forenses

Sección de Audio, Video y afines de Criminalística del Servicio Nacional De Medicina Legal y Ciencias Forenses

VI. Cooperación internacional

El auge de las tecnologías del último siglo ha traído consigo innumerables avances para la humanidad, pero también otra serie de retos para las autoridades, legisladores e investigadores, quienes han tenido que centrarse cada vez más en la persecución y sanción de los delitos cibernéticos, como la pornografía infantil, robo de identidad, acoso cibernético o "hacking". Según estimaciones de LACNIC, el organismo que maneja el Registro de Direcciones de Internet para América Latina y Caribe, el cibercrimen le cuesta a nuestra región alrededor de 90.000 millones de dólares al año6[6].

Dicho esto, la Fiscalía General del Estado cuenta con cooperación internacional con la finalidad de luchar contra los delincuentes cibernéticos. Por ejemplo, existe un vínculo de trabajo conjunto establecido junto a REMJA (Grupo de Trabajo en Delito Cibernético de las Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas).

VII. Capacitación

Debido a los retos excepcionales que presentan los delitos cibernéticos, la Fiscalía General del Estado en coordinaciones con otras unidades investigativas ha participado en diferentes programas de capacitación con la finalidad de que todos los participantes tengan la mayor cantidad de conocimiento y experiencia en el campo. Así, se han efectuado las siguientes capacitaciones:

- Delitos Cibernéticos de Tráfico de Vida Silvestre (V-WTCP). Capacitación auspiciada por el Departamento de Estado, el Servicio de Pesca y Vida Silvestre de EE. UU.

- Taller Subregional sobre Cooperación Internacional y Evidencia Digital. Taller auspiciado

5 Ecuador, Constitución de la República del Ecuador, Registro Oficial 449, 20 de octubre de 2008, art. 195.

6 Organización de Estados Americanos, "Ciberdelito: 90.000 millones de razones para perseguirlo", OEA, accedido 24 de octubre de 2021 https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-063/16.

por la Oficina de las Naciones Unidas contra la Droga y el Delito, UNODC

- Primer Curso de Especialización en Ciberseguridad y Cibercrimen. Curso auspiciado por la Dirección Nacional de Ciberdelitos de la Policía Nacional

Estas capacitaciones tienen la finalidad de bridar un gran aporte a la investigación de los delitos cibernéticos. Están basadas en un enfoque holístico que incorpora los siguientes tres aspectos:

1. Investigación: Este aspecto se enfoca en analizar las diferentes técnicas de análisis de evidencia, cómo combinar métodos de investigación tradicional con nuevas tecnologías.

2. Presentación de Evidencia: Este aspecto viene a ser la forma de cómo presentar la evidencia en una corte judicial.

3. Evaluación y análisis: Este aspecto se enfoca en cómo analizar la evidencia que es presentada, asegurarse de que la misma no ha sido alterada y conectar leyes existentes con crímenes modernos.

VIII. Proyección de la Fiscalía General del Estado frente a los ciberdelitos

En el marco de elementos asociados a la cooperación internacional, la Fiscalía General del Estado resaltó la importancia de contar con un instrumento que permita hacer frente a las graves y múltiples dificultades en materia de cibercrimen. De este modo, se consideró la necesidad de que el Ecuador se adhiera al Convenio de Budapest. En este sentido, el Ministerio de Relaciones Exteriores y Movilidad Humana de Ecuador manifestó a la Secretaría del Consejo de Europa el interés nacional para adherirse a dicho instrumento; sin embargo, la Secretaría señaló que el país debía tener en cuenta lo siguiente:

1. Contar con la legislación que penalice la ciberdelincuencia, además de existir el derecho procesal que otorgue a las autoridades policiales las facultades para investigar y obtener evidencia.

2. Una vez que se cuenta con dicha legislación, el Gobierno deberá enviar una carta al Secretario General del Consejo de Europa expresando su interés de adhesión.

3. La solicitud es puesta en consideración de las partes y posteriormente se enviará al Ecuador la carta oficial con la invitación para acceder a este instrumento. En este mismo contexto, es de gran valía e importancia que el país forma parte de la Red 24/7 a fin de mejorar el desempeño en el marco de las investigaciones penales y solicitudes internacionales de preservación de pruebas.

Así, se han realizado varias reuniones interinstitucionales. En efecto se han mantenido gestiones entre el Ministerio de Gobierno y la Fiscalía General del Estado Ecuatoriano, bajo la coordinación de Cancillería. Todo ello con el apoyo de la cooperación no reembolsable del Consejo de Europa y expertos de Glacy+. El fin es llegar a estructurar los siguientes documentos:

1. Análisis comparativo de legislación en ciberdelincuencia de Ecuador frente a otros países de la región.

2. Recomendaciones de reformas legales para ser presentadas ante la Asamblea Nacional.

Como punto final y no menos importante, la Fiscalía General del Estado gestiona y trabaja en la creación de la Unidad Especializada Contra la Ciberdelincuencia, con personal debidamente

capacitado en esta área. De esta manera, será posible trabajar de mejor manera antes estos delitos cibernéticos.

Si los países no toman en serio el crecimiento de criminalidad informática y no se preparan adecuadamente para contrarrestar este tipo de conductas delictivas, podrían sucumbir ante el avance incontrolable de este fenómeno. El Ecuador debe ir a la par de otros países y empezar a tomar decisiones, medidas y todas las acciones necesarias, en función de prepararse para la actualidad y el futuro. De este modo, no quedará al margen de situaciones que podrían afectar significativamente con la sociedad de la información ecuatoriana.

Referencias bibliográficas

Ecuador. Constitución de la República del Ecuador. Registro Oficial 449, 20 de octubre de 2008.

Ecuador Fiscalía General del Estado. "¡Tenga cuidado!, con un solo 'clic' podría caer en la red de los delitos informáticos". Fiscalía General del Estado, 22 de noviembre de 2015. https://www.fiscalia.gob.ec/tenga-cuidado-con-un-solo-clic-podria-caer-en-la-red-de-los-delitos-informaticos/.

Ecuador Ministerio de Telecomunicaciones y de la Sociedad de la Información. Política de Ciberseguridad. Quito: Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

Organización de Estados Americanos. "Ciberdelito: 90.000 millones de razones para perseguirlo". OEA, accedido 24 de octubre de 2021 https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-063/16.

FGE

FISCALÍA GENERAL DEL ESTADO

ECUADOR

Número de edición 030
ISSN: 2661-6920
Direccón: Juan León Mera N19-36 y Av. Patria
Edificio Fiscalía General del Estado. Piso 6
Teléfono: (02) 3985 800 Ext. 173037
Mail: estudiospenales@fiscalia.gob.ec

Fiscalía General del Estado
Dirección de Estudios Penales
Quito - Ecuador