Revista Judicial, Poder Judicial de Costa Rica, Nº 126, págs 220-225 ISSN 2215-2385 / junio 2019

EL ESPECTRO ACTUAL DE LOS DELITOS INFORMÁTICOS

MSc. Patricia Bonilla Rodríguez *
pbonilla@Poder-Judicial.go.cr

.

RESUMEN:

La informática llegó y se quedó. Este constante progreso tecnológico que experimenta la sociedad, supone una evolución en las formas de delinquir, dando lugar, tanto a la diversificación de los delitos tradicionales como a la aparición de nuevos actos ilícitos. Esta realidad ha originado la necesidad de distinguir los delitos informáticos de los demás. La conjugación de la ciencia de la ingeniería informática con la ciencia social del derecho, ha llevado, desde el punto de vista penal, a la evolución en nuevas formas de delinquir, o bien, a la "reestructuración" de conductas ya existentes, creando desde hace más de una década el concepto de "delito informático", siendo que, posterior a ello nace el "ciber-delito", el cual se diferencia del anterior por la incorporación del uso del Internet en la actividad criminal.

PALABRAS CLAVE: *Derecho Informático, Ciberdelincuencia, Ciberdelitos, Delitos Informáticos, Cibercrimen, Estafa Informática, Sabotaje Informático.*

ABSTRACT:

The computer came and stayed. This constant technological progress experienced by society, implies an evolution in the forms of crime, giving rise to both the diversification of traditional crimes and the appearance of new unlawful acts. This reality has led to the need to distinguish computer crimes from others. The combination of the science of computer engineering with the social science of law, has led, from the criminal point of view, to the evolution in new forms of crime, or to the "restructuring" of existing behaviors, creating from more than a decade ago the concept of "computer crime", being that, after that is born the "cyber-crime", which differs from the previous one by the incorporation of the use of the Internet in criminal activity.

KEYWORDS: *Computer Law, Cybercrime, Cybercrime, Cybercrimes, Computer Crimes, Cybercrime, Computer Fraud, Computer Sabotage.*

Recibido 23 de noviembre de 2018 **Aceptado 14 de febrero de 2019**

* Máster en Administración de Recursos Informáticos, Licenciada en Derecho e Ingeniera de Sistemas.

La informática llegó y se quedó. Actualmente nos rendimos ante los progresos tecnológicos, cada vez son menos las tareas manuales. El mundo cambia a una velocidad vertiginosa. En el pasado podíamos tener una alta certeza de que nadie podía acceder a información sobre nuestras vidas privadas. La información era solo una forma de llevar registros. Eso ya no es así, nuestra intimidad y privacidad está en constante amenaza y riesgo, la información sobre nuestra vida personal se está volviendo un bien muy cotizado por la mercadotecnia. Cada vez más y más personas tienen acceso a esta información, sin que las legislaciones sean capaces de regularlos. Este constante progreso tecnológico que experimenta la sociedad, supone una evolución en las formas de delinquir, dando lugar, tanto a la diversificación de los delitos tradicionales como a la aparición de nuevos actos ilícitos. Esta realidad ha originado la necesidad de distinguir los delitos informáticos de los demás.

El derecho como ciencia social, tiene por objeto el estudio de las normas jurídicas que, regulan y rigen la conducta del ser humano que vive en una sociedad.

Por otra parte, la cibernética es conocida como una ciencia multidisciplinaria, dado la relación que se da con otras áreas, sin embargo, está íntimamente asociada a la tecnología, que forma parte de la ciencia de la ingeniería, donde mediante conocimientos científicos y tecnológicos se logra la innovación, la invención, y el desarrollo de técnicas que permiten satisfacer las necesidades de la sociedad.

Esta conjugación de "*ciencias*", ha llevado, desde el punto de vista penal, a la evolución en nuevas formas de delinquir, o bien, a la "*reestructuración*" de conductas ya existentes, creando desde hace más de una década el concepto de "*delito informático*", siendo que, posterior a ello nace el "*ciber-delito*", el cual se diferencia del anterior por la incorporación del uso del Internet en la actividad criminal.

En Costa Rica, los delitos informáticos, empiezan a normarse a partir del año 2001, con la promulgación de la Ley 8148, en la cual se adicionan al Código Penal, los artículos de Violación de comunicaciones electrónicas (196 bis), Fraude Informático (217 bis) y Alteración de datos y sabotaje informático (229 bis).

En el año 2012, se promulga la Ley No. 9048, denominada "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal", la cual vino a modificar los artículos 167, 196, 196 bis, 214, 217 bis, 229 bis y 288 del Código Penal, donde los cambios se dieron principalmente en el aumento de las penas, y se incluyeron conductas relacionadas con el uso de redes sociales, medios informáticos, entre otros.
Por otra parte, se adicionó un inciso 6) al Artículo 229, correspondiente al "Daño Agravado", ubicado en el Título correspondiente a los "Delitos contra la propiedad", donde también se incorpora, un artículo 229 ter, correspondiente al "Sabotaje Informático".

Por último se agregó la "*Sección VIII*" al Título VII de los "*Delitos contra la Propiedad*", denominada "Delitos Informáticos y conexos", los cuales regulan temas como suplantación de identidad (230), Espionaje Informático (231), Instalación o propagación de programas informáticos maliciosos (232), Suplantación de páginas electrónicas (233), Facilitación del delito informático (234), Narcotráfico y Crimen Organizado (235) y Difusión de información falsa (236).

En relación con las normas citadas en el párrafo anterior, pareciera que lo ideal hubiese sido crear un nuevo título en el Código Penal, donde se incluyeran los "*Delitos Informáticos y conexos*". Esto por cuanto los bienes jurídicos tutelados en él no son exclusivos de los "Delitos contra la Propiedad".

Otro aspecto que, resulta necesario e importante tener en consideración cuando se trata el tema de "delitos informáticos", es que existe una

clasificación, donde, por un lado, la informática es utilizada como medio para la realización de la acción delictiva, y por otro, cuando la informática es el objeto de la acción delictiva.

La informática es utilizada como medio para llevar a cabo la actividad delictiva como por ejemplo, en delitos sexuales (pornografía, seducción o encuentro con menores por medios electrónicos), delitos contra el ámbito de la intimidad (violación de correspondencia o comunicaciones), delitos contra el ámbito de la identidad (suplantación de identidad, violación de datos personales), delitos contra la propiedad (extorsión informática, estafa informática), delitos económicos (espionaje informático), delitos contra la seguridad de la nación (espionaje), etc.

Ahora bien, la informática es utilizada como objeto de la acción delictiva, cuando la integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos (entiéndase que un sistema incluye, hardware, software, redes telemáticas, etc.), son vulnerados, atacados, siendo el blanco de la delincuencia. Ejemplo de esta clase de delitos informáticos son el sabotaje informático, el daño informático, la instalación o propagación de programas informáticos maliciosos, la suplantación de páginas electrónicas y la facilitación del Delito Informático.

De lo anterior, surge la interrogante, ¿será oportuno clasificar como delito informático aquellos delitos que usan como medio las tecnologías de la información? Actualmente, la mayoría de los delitos son realizados utilizando un elemento informático, por lo tanto, cada vez sería mayor la cantidad de conductas que se catalogarían en ese sentido, por tanto, pareciera que lo correcto sería clasificar un delito como tal cuando la informática sea el objeto de la acción delictiva, y no el medio para llevarlo a cabo.
Ahora bien, lo que sí debe tenerse en cuenta es que, tanto los delitos cometidos por medios informáticos, o bien como objeto de la actividad delictiva, tienen en común las siguientes características:

De rápida ejecución y alto alcance: Esta clase de delitos puede ser realizados de forma sumamente rápida. Solo se requiere pocos procedimientos, ejecutados a través de un clic, y su alcance puede ser de una a miles de personas afectadas, incluso en diferentes países.

De fácil encubrimiento: La misma tecnología permite cubrir la acción, haciéndolos difíciles de detectar. Muchas veces las personas afectadas lo pueden confundir con fallas en sus sistemas, por lo que, a la hora de querer arreglarlo, podrían más bien alterar la prueba requerida para comprobar el ilícito.

Son novedosos: Muchos de los Delitos Informáticos tienen la particularidad de ser novedosos, de reciente creación, con un alto grado de imaginación y creatividad.

No siempre son fáciles de tipificar: debido a su complejidad a la hora de determinar si se está ante un nuevo delito, o bien, si se trata de conductas ya reguladas.

Bien jurídico tutelado: Esta clase de delitos trae consigo la protección a nuevos bienes jurídicos tutelados, tal como el de la información.

Los datos informáticos son intangibles: En los delitos informáticos los daños causados son intangibles, y a eso sumaría que son difíciles de cuantificar.

Los datos informáticos son difíciles de vigilar: Por las elevadas cantidades de información, la gran variedad de sistemas, redes informáticas, falta de expertos en la materia, los déficits en el control, todo ello dificulta la vigilancia y el poder identificar y controlar las operaciones ilegales en la red. Es decir, es difícil contar con expertos que podrían denominarse "guardianes" o "policías" de la información. Muchos países ya están optando por tener sus propios "ciber-ejércitos".
Los datos informáticos son transitorios por naturaleza: El tiempo es un factor importante en la investigación de los Delitos Informáticos, las

medidas deben ser lo suficientemente rápidas para la recolección de pruebas, mientras la información relevante está aún disponible.

En cuanto a los bienes jurídicos tutelados en *esta clase de delitos se consideran como tal, la "Información"*, entendiéndose esta de forma amplia, involucrando en ella, documentos, bases de datos, expedientes electrónicos, cuentas bancarias, información médica, información industrial, etc., la cual de violentarse, podrá influir de forma transcendental en la vida de un individuo o de la colectividad, y conforme con el impacto presentado, podrá transgredir sustancialmente el desarrollo económico de uno o varios países, pudiendo llegar en pocos minutos a la catástrofe internacional.

En lo que respecta a *"Internet"*, la jurisprudencia de la Sala Constitucional, por ejemplo en resolución número 10627-2010, del dieciocho de junio del año dos mil diez, ha señalado que el bien jurídico tutelado, no es la red como tal, sino el derecho a la comunicación y el derecho a la información, pudiendo incluirse acá, el derecho al conocimiento, los cuales son proveídos por Internet. Por lo tanto, a partir de ello, se obtiene, además de la Información, dos bienes jurídicos adicionales: la Comunicación y el Conocimiento. Es por las características anteriores, que la investigación, persecución y judicialización de los delitos informáticos, ha incidido en la forma en que se desarrollan algunos actos del proceso penal, lo que ha llevado a algunos países como México, Portugal, República Dominicana y Ecuador, a realizar reformas en su Código Procesal Penal, incorporando actos procesales especializados, como lo son la conservación o preservación expedita de los datos, decomiso de datos informáticos, responsabilidad del custodio, confidencialidad del proceso investigativo, reconocimiento de grabaciones, acciones encubiertas, entre otros.

En el caso costarricense, nuestro Código Procesal Penal ha permitido realizar las acciones anteriores, sin necesidad de cambios normativos, lo cual no limita a que se realice un estudio que determine una mejora en nuestra legislación.

Otros aspectos que deben definirse, están relacionados con la competencia territorial, donde se está en presencia de delitos de carácter transnacional, por lo que la armonización de las legislaciones, es de vital importancia, así como el potenciar el uso de instrumentos de cooperación internacional en la materia, tal como el Convenio de Budapest, ratificado por Costa Rica en el año 2017. También, estas actividades delictivas vienen a modificar aspectos de carácter de índole espacial y temporal de los hechos, los cuáles deben ser analizados bajo nuevos parámetros.

Ahora bien, dentro de todo el proceso penal, la obtención y conservación de la prueba es un elemento básico para lograr la verdad de los hechos. Es por ello, que en aquellas actividades delictivas donde ha mediado un elemento tecnológico o bien, la tecnología es el objeto de ésta, el tema de la "evidencia digital" reviste una especial importancia, por las características propias del elemento informático, que lo dificultan.

La obtención adecuada de este tipo de evidencia incide en la calidad probatoria, dado que, ésta puede ser comprometida, tanto física como lógicamente, al ser destruida, dañada, borrada, alterada, etc., razón por la cual, la metodología utilizada en el manejo, sistematización de la identificación, adquisición, análisis y preservación de la evidencia digital, reviste de especial importancia en la época actual, donde sin duda la "Informática Forense" es un elemento fundamental en todo este proceso.

Se estima necesario contar con guías, procedimientos, leyes, etc., que salvaguarden su integridad, tanto en su recolección, preservación y en el manejo de la cadena de custodia.

Parece oportuno también, lograr procesos de capacitación, continuos y adecuados para todas las partes que participan en ellos, de forma tal que,

durante las audiencias se tenga claro el lenguaje técnico básico, así como, aspectos fundamentales para la comprensión de esta clase de delitos.

También es necesario la creación conjunta de procedimientos, normativa, etc., para estandarizar la forma en que se da tratamiento a la "evidencia digital", así como de otras posibles actuaciones relacionadas con ello.

Si bien es cierto, por más de 30 años el OIJ ha investigado estos delitos, siendo pioneros al crear desde esa época la Sección de Delitos Informáticos, pareciera necesario que esa experiencia acumulada, debe ser canalizada y evolucionar, en la creación de un "Centro Policial Cibernético", que cumpla diversos roles, tal como: a) ser el centro de investigación en delitos informáticos, con las técnicas de informática forense de vanguardia en la región, b) ser el centro de capacitación en delitos informáticos a nivel regional y, c) ser el centro innovador en la identificación de nuevas modalidades delictivas en la materia.

También se hace necesario analizar la normativa sustantiva y procesal de estos delitos a efectos de promover proyectos de ley, que permitan un mejor abordaje, y poder asumir nuevos retos de investigación, como lo son los elementos biométricos, el uso de drones, robótica, inteligencia artificial, entre otros, y muchos que aún desconocemos que pronto surgirán.

La ciberdelincuencia llegó y crece día con día por lo que, el Derecho debe evolucionar, y buscar los mecanismos necesarios para avanzar con mayor celeridad.

REFERENCIAS BIBLIOGRÁFICAS.

Miró Llinares, Fernando. El Cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Editorial Marcial Pons. 2012

Flore Prada Ignacio. Criminalidad Informática. Aspectos sustantivos y procesales. Editorial Tirant Monografías, 2012

Ortiz Pradillo, Juan Carlos. Problemas Procesales de la Ciberdelincuencia. Editorial Colex, 2013.

Sanchez Fallas, Francisco. La tramitación de los Procesos Penales. Escuela Judicial. 2009

Ministerio Público. 81 términos prácticos para comprender el proceso penal de Costa Rica, en Lenguaje no jurídico. https://ministeriopublico.poder-judicial.go.cr/media/attachments/2018/05/28/manual-terminos-practicosmp.pdf

Casco Maria Eugenia, Roatta, S. Fogliato, G. El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012 http://sedici.unlp.edu.ar/handle/10915/46243

Andrade Roberto, La Administración de la Evidencia Digital. https://es.linkedin.com/pulse/la-administraci%C3%B3n-de-evidencia-digital-roberto-andrade

Bonilla Rodríguez Patricia. Tesis de Grado "Limitaciones Jurídicas y Policiales en la investigación y persecución de los delitos informáticos", 2013