DELITOS INFORMÁTICOS:

PRIMERA APROXIMACIÓN A UNA PROBLEMÁTICA TRANSNACIONAL

Dra. Anabella Calió

Resumen – Frente a las nuevas tendencias globales vinculadas con el avance y el empleo de forma habitual de las tecnologías - tanto por personas físicas como jurídicas y entidades gubernamentales – existe una exposición evidente a la utilización maliciosa de dichas herramientas por parte de ciberdelincuentes y organizaciones criminales. Es por ello, que el presente artículo tiene como objeto efectuar un recorrido sobre las nociones generales que comprenden a los delitos informáticos y un estudio de los instrumentos legales que dan tratamiento a la temática, tanto a nivel supranacional como interno.

Palabras clave – *delitos informáticos, transnacionalidad, nuevas tecnologías, regulación.*

1. Introducción - La masificación de manera exponencial de las nuevas tecnologías de la información y la comunicación (TIC) dentro de la sociedad moderna, ha traído aparejado consigo el surgimiento de diversos delitos que se sirven de éstas para su comisión. Es por ello, que los Estados se enfrentaron a la necesidad de sancionar leyes que les otorguen tipicidad, antijuridicidad y culpabilidad a dichas acciones, tanto a nivel nacional como supranacional. A los fines de desarrollar la temática que nos atañe, es preciso resaltar algunas cuestiones que permitan delimitar el alcance de los delitos informáticos.

Para comenzar, cabe destacar que no existe una única conceptualización aceptada por los juristas con relación a dicha problemática. No obstante, muchos de ellos coinciden en que el ciberdelito es una conducta reprochable en la cual interviene un

dispositivo informático como medio o fin en la comisión de la acción antijurídica. El primero de ellos implica que los ciberdelincuentes se sirven de cualquier herramienta tecnológica como método para la comisión del acto ilícito, como el *grooming*. El segundo, supone que la maniobra delictuosa tiene como objetivo de generar daños a artefactos informáticos, como los daños a programas o datos computarizados.

Las innovaciones digitales atraviesan transversalmente a cualquier conducta tipificada en el Código Penal y leyes complementarias dado que, actualmente, la tecnología se encuentra presente en cualquier arista de nuestras vidas. En relación con ello, existen figuras penales creadas a partir del surgimiento de las nuevas tecnologías y que, en ausencia de estas, no podrían llevarse a cabo, tal como ocurre con el *phishing*. No obstante, también existen delitos tipificados en el Código Penal que subsistirían sin la utilización de medios tecnológicos, pero se sirven de estos para su comisión.

2. Carácter transnacional

Este tipo de conductas poseen ciertas características que las diferencian notablemente de otros delitos, tales como su facilidad de comisión y propagación, su anonimato y su inmediatez. Sin embargo, la más saliente de ellas es, sin duda, su carácter transnacional. Se trata de actos de difícil delimitación geográfica, dado que sus conductas preparatorias pueden iniciarse en un país y casuar efectos en otros Estados.

Lo mencionado se debe a diversos factores, entre ellos, la innegable velocidad de la red que facilita la expansión inmediata de cualquier tipo de hecho delictivo mediante el acceso a datos que se encuentran almacenados en sistemas o equipos diversificados por todo el mundo. Asimismo, y en consonancia con la definición esbozada con anterioridad, existen delitos internacionales que eran ejecutados con anterioridad a la masividad tecnológica que nos atraviesa y que, en la actualidad, se sirven de estas nuevas herramientas para cometerlos de forma más rápida, anónima, y eficaz; entre ellos, podemos mencionar el *ciberterrorismo*.

En este sentido, los sujetos activos del mencionado delito utilizan herramientas que les proveen las nuevas tecnologías con el objetivo de ocasionar daños o perjuicios a otras naciones. En efecto, se puede advertir como los sujetos pasivos de los ciberdelitos pueden ser tanto personas físicas como

personas jurídicas y hasta entes gubernamentales. De aquí deviene uno de los aspectos que denotan la importancia de la cooperación entre los países en materia de ciberdelitos, y es por ello que, se debe percibir, analizar y atacar este fenómeno como una problemática internacional.

En virtud de lo expuesto, Gómez Vieites (2019) afirma que, en una era marcada por las nuevas tecnologías, las sociedades modernas poseen una dependencia cada vez mayor a los sistemas informáticos para el control de muchos procesos y actividades cotidianas, tales como, el control del fluido eléctrico, de las centrales de conmutación telefónicas, del tráfico aéreo, de los sistemas financieros, entre otros. Por este motivo, el autor sostiene que se podría colapsar por completo el funcionamiento de un país desarrollado si se dañasen algunos de sus principales redes y sistemas informáticos. Al respecto, podemos colegir que, los futuros conflictos de intereses y bélicos entre naciones podría manifestarse a partir de ataques cibernéticos.

3. Cooperación Internacional

El primer continente que comenzó a adoptar acciones tendientes a crear estándares para la persecución de los delitos cibernéticos ha sido el europeo -ejemplo por excelencia de la integración supranacional-es por ello que, en el año 2001, se crea el Convenio sobre la Ciberdelincuencia en el seno del Consejo de Europa, firmado en Budapest, con motivo de la celebración de la Conferencia Internacional sobre la Ciberdelincuencia. Dicho instrumento cuenta con la firma de más de 50 países y fue ratificado por la República Argentina el día del 05 de junio de 2018.

En tenor a lo esbozado en su preámbulo, persigue como objeto *"(…) llevar a cabo una política penal común destinada a prevenir el delito en el ciberespacio y, en particular, de hacerlo mediante la adopción de una legislación apropiada y la mejora de la cooperación internacional".* En otros términos, busca armonizar las legislaciones de los países a partir de una serie de recomendaciones en materia penal y procesal penal para la persecución de este tipo de conductas.

El Convenio de Budapest se puede dividir en dos partes: la primera de ellas -que comprende los artículos 1 al 13- aborda nociones de Derecho Penal Internacional y, la segunda parte -conformada por los artículos 14 al 35- hace referencia al Derecho Procesal

Penal Internacional. Es por este motivo que, en su primer capítulo, efectúa una armonización sustantiva de los términos que serán mencionados a lo largo del Convenio y sienta las bases de una terminología común para todos los Estados.

Por otra parte, en el segundo capítulo del documento, se establecen las medidas que los Estados firmantes deben adoptar en el ámbito regulatorio nacional, requiriendo a éstos la sanción de las siguientes conductas ilícitas:

I. Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:
   a. Acceso ilícito.
   b. Interceptación ilícita.
   c. Atentados contra la Integridad de los datos.
   d. Atentados contra la Integridad del sistema.
   e. Abuso de equipos e instrumentos técnicos.

II. Infracciones informáticas:
   a. Falsedad informática.
   b. Estafa informática.

III. Infracciones relativas al contenido:
   a. Infracciones relativas a la pornografía infantil.

IV. Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines.

De igual modo, el Convenio ajusta parámetros en relación con la tentativa y la complicidad en los ciberdelitos, así como también, el supuesto de que el sujeto activo sea una persona jurídica. Asimismo, en su artículo 35 compele a los Estados firmantes a la creación de un Centro de Respuestas localizable las 24 horas del día los siete días de la semana, con el fin de asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos; ello no resulta una cuestión menor dado que, en materia de ciberdelincuencia, no existe una gran tasa de denuncias y, al mismo tiempo, la persecución de los delitos debe ser inmediata.

Por otra parte, destina un apartado al tratamiento de la competencia esbozando que, será competente el Estado cuando la infracción haya sido cometida en su territorio; a bordo de una nave que enarbole el pabellón de ese Estado; a bordo de una aeronave inmatriculada en ese Estado. Ello, si la infracción es punible penalmente en el

lugar donde se ha cometido o si la infracción no pertenece a la competencia territorial de ningún Estado. Dicho aspecto ha sido crucial toda vez que, al tratarse de un delito carente de barreras geográficas que lo delimiten, la jurisdicción y legislación aplicable resultaba un debate recurrente.

Asimismo, dedica un artículo a hacer mención sobre la extradición de los ciberdelincuentes siempre que las conductas resulten punibles por la legislación de los dos Estados implicados y tengan prevista una pena privativa de libertad de una duración mínima de un año -al igual que ocurre en la legislación nacional-.

4. Regulación: derecho comparado

4.1. El caso de España

El Código Penal Español sancionado en 1995, ha regulado una serie de conductas antijurídicas contra la ciberdelincuencia. En ese sentido, tipificó hechos cometidos mediante o en contra de objetos informáticos -tal cual surge de la definición de ciberdelitos esbozada al comienzo de la presente ponencia-. La técnica utilizada por el legislador para la persecución de dichas conductas fue la de modificar y extender el ámbito de aplicación de los delitos tradicionales que podrían ser cometidos a través de las nuevas tecnologías.

Al respecto, Salvadori, I. (2011) advierte que la extensión de los tipos delictivos clásicos fue realizada de dos maneras. Por una parte, se introdujo dentro de los delitos tradicionales subtipos autónomos para castigar las nuevas modalidades ilícitas. Y por la otra, se amplió el ámbito de los objetos materiales de aquellos delitos que presentaban analogías con los nuevos hechos delictivos. Sin embargo, en la modificación del Código Penal Español en el año 2010 se han introducido nuevos delitos de daños informáticos dentro de un tipo penal autónomo -en su artículo 264- subsanando, de esta manera, la decisión tomada por el legislador en el año 1995, en sus esfuerzos por integrar y adaptar los nuevos delitos informáticos a los tipos delictivos tradicionales.

4.2. El caso de Alemania

Alemania, al igual que Italia, y en contraposición con el Código Penal Español del año 1995, ha decidido legislar tipos delictivos autónomos que regularan estas conductas ilícitas. En tal sentido, en dicho Estado los ciberdelitos se encuentran legislados en diversas normativas; entre ellas,

la Ley de Seguridad Informática alemana (ITSicherheitsgesetz) de 25 de julio de 2015, que modificó una serie de leyes, en particular la Ley de Telemedia alemana (Telemediengesetz), la Ley de Telecomunicaciones alemana (Telekommunikationsgesetz), la General de la UE Reglamento de Protección de Datos (Datenschutz-Grundverordnung), la Ley Federal de Protección de Datos de Alemania (Bundesdatenschutzgesetz) y la Ley de la Oficina Federal de Seguridad de la Información (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik). (Arles Gamba Velandia, J., 2019)

4.3. El caso de Colombia

En el marco del análisis de la regulación colombiana, se puede encontrar una influencia del Convenio de Budapest en los tipos penales descritos en el Título VII Bis del Código Penal incluyendo en él las infracciones detalladas en el primer capítulo del instrumento internacional desarrollado de forma precedente.

La Ley 1.273 vigente desde el año 2009 regula los delitos informáticos en dicho Estado -legislación complementaria al Código Penal Colombiano- que crea un nuevo bien jurídico tutelado a partir del concepto de la *protección de la información y de los datos*, con el cual se preserva integralmente a los sistemas que utilicen las tecnologías de la información y las comunicaciones. En este orden de ideas, la mencionada ley persigue los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. A partir de la Ley 1273 de 2009, se tipificaron los siguientes delitos informáticos: acceso abusivo a un sistema informático; obstaculización ilegítima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios *web* para capturar datos personales y transferencia no consentida de activos. (Ojeda Pérez, J.; Rincón Rodríguez, F.; Arias Flórez, M.; Daza Martínez, L., 2010)

5. Regulación: legislación nacional

El ordenamiento jurídico argentino fue incorporando y modificando la legislación vigente a los fines de hacer frente a los delitos cibernéticos, sancionándose, de este modo, la Ley de Delitos Informáticos Nº

26.388; Ley de Piratería Nº 25.036; Ley de "Grooming" N° 26.904; Ley de Protección de Datos Personales N° 25.326; Ley de Calumnias e Injurias Nº 26.551.

En virtud de la sanción de la Ley N° 26.388 en el año 2008, se reforma el Código Penal de la Nación Argentina, con el objeto de incorporar nuevos artículos que den tratamiento a los delitos informáticos. En esa inteligencia, se realizó una modificación al artículo 77 ampliándose, de este modo, el alcance de la terminología de "documento" -entendiendo como documento a toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión-; "firma" y "suscripción -incorporando los supuestos de que sean efectuadas mediante medios digitales-; "instrumento privado" y "certificado" -aún los firmados digitalmente-.

Asimismo, el artículo 2 de la Ley modifica el Código Penal en su artículo 128 referente al delito de pornografía infantil -apartado que se encontraba legislado en la Convención sobre la Ciberdelincuencia celebrado en Budapest- señalando que será penada la divulgación, comercialización, publicación -entre otros- de la representación de un menor de 18 años que se hiciere por cualquier medio. De igual modo, se añade al artículo 153 del Código Penal todo acceso, apoderamiento, supresión, desviación, intercepción o captación indebida de una comunicación electrónica o telecomunicación proveniente de cualquier sistema de carácter privado o de acceso restringido; como así también a quien accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido -situación también regulada dentro de la mencionada Convención de Budapest-.

Por último, mencionaremos el artículo 8 sustituyendo el artículo 157 bis del Código Penal, reprimiendo al que viole ilegítimamente sistemas de confidencialidad y seguridad de datos o accediere, de cualquier forma, a un banco de datos personales; al que ilegítimamente proporcionare o revelare a otro, información registrada en un archivo o en un banco de datos personales, cuyo secreto estuviere obligado a preservar por disposición de la ley; al que ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales; ello, sin perjuicio de la legislación específica en

materia de protección de datos que se desarrollará seguidamente-.

Para concluir con dicha normativa, y en términos generales, la legislación equipara las correspondencias con las comunicaciones llevadas a cabo a través de medios electrónicos dado que, a la luz de la realidad que nos atraviesa, la mayor parte de las comunicaciones se efectúan a través de este medio.

El principio general de la Ley de Protección de Datos Personales es que cualquier tratamiento de datos personales debe ser consentido específicamente por el interesado. Dicho consentimiento debe otorgarse libremente, en función de la información proporcionada previamente al interesado (informado) y expresada por escrito o por medios equivalentes, dependiendo de cada caso. El interesado puede revocar el consentimiento en cualquier momento, aunque esto no tendrá un efecto retroactivo. (Arles Gamba Velandia, J., 2019)

Por su parte, la Ley N° 26.904 incorpora como artículo 131 del Código Penal el ciberdelito de Grooming, entendiendo a éste como el acto mediante el cual, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, una persona contactare a un menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma. En este sentido, conforme se desprende de la tipificación detallada, la acción antijurídica se el contacto a través de medios tecnológicos a un menor de edad con fines sexuales -delitos tipificados entre los artículos 118 a 133 dentro del Código Penal Argentino-.

Las leyes mencionadas han pretendido dar tratamiento a las diversas formas de manifestación de los delitos cibernéticos. Sin perjuicio de ello, las nuevas tecnologías poseen un dinamismo ineludible, encontrándose en constante y veloz cambio, haciendo dificultoso producir una legislación apropiada que se encuentre a la altura de los requerimientos en todo momento.

6. Reflexiones finales

En suma, la delincuencia informática resulta el *modus operandi* elegido por diversos criminales y organizaciones delictivas transnacionales para la comisión de conductas antijurídicas, con fines diversos, por su inminencia y eficacia, así como también, por su rápida expansión y anonimato. De igual manera, la mayoría de nosotros contamos con un aparato

tecnológico en nuestras manos, guardando en él hasta la información más sensible y emitiendo datos al ciberespacio a un ritmo vertiginoso. Es por ello que, el uso deliberado de las mismas, en ocasiones sin conocer acabadamente los riesgos que implican, nos convierte en un objetivo asequible a los ojos de los ciberdelincuentes.

Para finalizar, y tal como se indicó en un comienzo, este artículo es la primera entrega de las que se irán analizando con nuestros lectores; y dejo planteada para la próxima ponencia el desarrollo de la temática de ciberdelitos y su vinculación con las entidades bancarias o emisoras de tarjetas.

Referencias bibliográficas

- Arles Gamba Velandia, J. (2019). *El delito informático en el marco jurídico colombiano y el derecho comparado: caso de la transferencia no consentida de activos.* Facultad de Derecho, Universidad Exterando De Colombia. Recuperado de https://bdigital.uexternado.edu.co/bitstream/001/2728/1/GUAAA-spa-2019-El_delito_informatico_en_el_marco_juridico_colombiano_y_el_derecho_comparado

- Díaz Gómez, A. (2010). *El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest.* Universidad de La Rioja. Revista REDUR 8.

- Gómez Vieites, A. (2019). *La lucha contra el ciberterrorismo y los ataques informáticos.* Recuperado de: https://www.edisa.com/wp-content/uploads/2019/08/la_lucha_contra_el_ciberterrorismo_y_los_ataques_informaticos.pdf

- Hernández Díaz, L. (2009). *El delito Informático.* San Sebastián: Revista Eguzkilore. Número 26. Recuperado de: https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf

- Ojeda Pérez, J.; Rincón Rodríguez, F.; Arias Flórez, M.; Daza Martínez, L. (2010). *Delitos informáticos y entorno jurídico vigente en Colombia.* Bogotá: Cuadernos de Contabilidad, vol. 11, N° 28. Recuperado de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

- Salvadori, I. (2011). *Los nuevos delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5/2010. Perspectiva de derecho comparado.* ADPCP, VOL. LXIV.