Ars Iuris Salmanticensis
TRIBUNA DE ACTUALIDAD
Vol. 8, 21-25
Diciembre 2020
eISSN: 2340-5155

La ciberdelincuencia en el contexto de la pandemia del coronavirus. Una aproximación desde el marco convencional

Cybercrime in the context of the coronavirus pandemic. An approach from the conventional framework

Roberto Carlos VILCHEZ LIMAY
Universidad Nacional Mayor de San Marcos

1. La pandemia de la COVID-19 obligó, a los Estados de cada país del mundo, a asumir políticas de aislamiento social y salubridad, a fin de evitar la propagación de este virus. Así, en el Perú, el Poder Ejecutivo estableció un estado emergencia nacional, mediante el Decreto Supremo n.º 044-2020-PCM, del 15 de marzo de 2020, el cual ha sido prorrogado a través de sendos decretos supremos; siendo que este aún se mantiene, con mayores o menores restricciones, conforme a zonas geográficas donde se han hallado índices elevados de contagio.

Bajo ese contexto, las relaciones sociales, económicas, laborales, etc., se desarrollan, con mayor frecuencia e intensidad, mediante el empleo de las tecnologías de la información y la comunicación (TIC); advirtiéndose que estas han propiciado que el fenómeno criminal de la ciberdelincuencia, también, se haya repotenciado, aprovechando el conocimiento técnico especializado, el rasgo de anonimato y los espacios clandestinos del ciberespacio por parte de los agentes delictivos.

En ese sentido, el presente escrito tiene como objeto describir la naturaleza dogmática de los ciberdelitos que se regulan en la legislación penal peruana, a fin de poder clasificarlos y establecer algunos criterios normativos para su mejor tratamiento en el proceso penal; así como resaltar la necesidad de incorporar nuevas figuras delictivas informáticas, conforme a las exigencias convencionales internacionales.

2. En primer término, consideramos que la ciberdelincuencia debe ser concebida como aquel fenómeno criminal que aborda los hechos y conductas dirigidos a vulnerar o poner en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos[1], los que tienen ocasión, a partir del desarrollo científico-tecnológico de la humanidad.

Conviene agregar que, dentro la ciberdelincuencia, también se ubican los eventos delictivos que, para su ejecución, emplean los sistemas informáticos, datos informáticos y las tecnologías de la información y la comunicación, siempre que estos ostenten un marco convencional de protección o se encuentren regulados como tal (instrumentos) en los tipos penales de cada legislación penal nacional.

3. Ahora bien, en lo atinente al marco convencional de lucha contra la ciberdelincuencia, resulta pertinente resaltar el Convenio de Budapest, del año 2001, el cual es un tratado internacional generado por los países miembros del Consejo de Europa, con la finalidad de combatir el fenómeno del cibercrimen, que contiene un modelo de legislación-tipo, el cual trasunta en mecanismos de homologación de normas de Derecho Penal sustantivo, estandarización de procesos penales y cooperación internacional.

Conviene anotar que el Perú, en el año 2014, solicitó suscribirse al precitado convenio; siendo que, en el año 2015, el Consejo Europeo aprobó dicho pedido. Posteriormente, el Congreso de la República, el 12 de febrero de 2019, aprobó el Convenio de Budapest, a través de la Resolución Legislativa n.º 30913, el cual fue ratificado por el Poder Ejecutivo, mediante el Decreto Supremo n.º 010-2019-RE, del 09 de marzo de 2019, estableciéndose el día 01 de diciembre de 2019 como fecha de entrada en vigor del Convenio sobre la ciberdelincuencia.

A continuación, procederemos a resaltar los delitos informáticos contenidos en la Ley n.º 30096 (Ley de delitos informáticos peruana) y otros ilícitos penales, que se encuadrarían dentro del marco de la ciberdelincuencia; así como la necesidad de incluir algunas modalidades delictivas previstas en el marco convencional que aún no ostentan una recepción normativa en la legislación penal peruana.

1. Esta definición la encontramos en el Preámbulo del Convenio sobre la Ciberdelincuencia, celebrado en Budapest, en el año 2001. Ver: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.

4. En la Ley n.º 30096, del 22 de octubre de 2013, se han previsto una serie de ilícitos penales que se encuadran dentro del fenómeno de la ciberdelincuencia.

4.1. Así, en el artículo 2 de la precitada ley, se regula el delito de «acceso ilícito», el cual implica ingresar, a todo o en parte, a un sistema informático, sin autorización de su titular o poseedor, vulnerando las medidas de seguridad dirigidas a impedirlo; además, en el artículo 3**,** se sanciona el ilícito penal de «ataque a la integridad de los datos informáticos», el cual comporta introducir, borrar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos, de forma deliberada e ilegítima. Asimismo, en el artículo 4, se prevé la figura delictiva de «ataque a la integridad del sistema informático», el que se caracteriza por volver inutilizable, total o parcialmente, un sistema informático, o impide, entorpece e imposibilidad el acceso, funcionamiento o prestación servicios de este.

Se puede identificar, también, el artículo 7, que reprime el hecho delictivo de «interceptación de datos informáticos», el cual consiste en intervenir datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos.

Finalmente, se aprecia el artículo 10 que prevé el ilícito penal de «abuso de mecanismos y dispositivos informáticos», el que implica fabricar, diseñar, desarrollar, vender, facilitar, distribuir, importar u obtener para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de otros ciberdelitos, o el que ofrece o presta servicio que contribuya a ese propósito.

4.2. Por otro lado, debemos indicar que la **Convención de Budapest del 2001**, en su artículo 7, regula y sanciona la conducta delictiva de «falsificación informática», la cual consiste en la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados, a efectos legales, como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Evento criminal que no posee un correlato normativo en la legislación penal peruana; por lo que se aprecia como menester plantear alguna propuesta de ley que busque incluirla.

A todo este catálogo de ciberdelitos se les puede denominar «delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos».

5. Por otro lado, aunque siempre en el marco de la ciberdelincuencia, se ubican los delitos que no solo afectan la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, sino, también, otros bienes jurídicos distintos como el **patrimonio**; la **indemnidad sexual**; la **fe pública**, etc.

5.1. Aquí, se ubica el hecho punible de proposiciones, a niños, niñas y adolescentes, con fines sexuales, por medios tecnológicos, previsto en el artículo 5 de la Ley n.º 30096, precepto que sanciona a quien, a través de las tecnologías de la información o

de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él; siendo que el mismo comportamiento será penado cuando la víctima posee entre catorce y menos de dieciocho años de edad, siempre que medie engaño.

Asimismo, en el artículo 8 de la ley precitada, se regula el delito de «fraude informático», reprimiendo a quien procura, para sí o para otro, un provecho ilícito en perjuicio de terceros mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático.

Además, también se prevé el delito de «suplantación de identidad», en el **artículo 9** de la Ley n.º 30096, sancionando a quien, mediante las tecnologías de la información o de la comunicación, suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral.

5.2. Por otro lado, resulta pertinente señalar que la legislación penal peruana ha omitido regular dos delitos informáticos importantes, tales como el de «infracción a la propiedad intelectual y derechos afines, mediante un sistema informático» y el de «ciber discriminación», los que ostentan un basamento normativo convencional, en el artículo 10 de la Convención de Budapest del 2001 y en el Protocolo Adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba, cometido por medio de sistemas informáticos, del año 2003 —respectivamente—. Por lo que se aprecia como necesaria la incorporación de estos hechos punibles al referido ordenamiento jurídico penal.

6. La ciberdelincuencia se muestra como un fenómeno criminal transversal a todas las figuras delictivas del sistema penal. Así, resulta paradigmático enunciar las referencias normativas que recibe esta en las convenciones internacionales contra el crimen organizado y los delitos de corrupción de funcionarios.

En la Convención de las Naciones Unidas contra la delincuencia organizada trasnacional y sus protocolos, conocida como la «Convención de Palermo», del año 2000, en su artículo 27, inciso 3, se prescribe que «Los Estados Parte se esforzarán por colaborar en la medida de sus posibilidades para hacer frente a la delincuencia organizada transnacional **cometida mediante el recurso a la tecnología moderna**».

Conviene anotar, además, que la Convención de las Naciones Unidas contra la corrupción, denominada «Convención de Mérida», del año 2003, en su artículo 48 (Cooperación en materia de cumplimiento de la ley), inciso 3, establece una regla semejante a la descrita ut supra; apreciándose, de esta manera, por parte de las agencias estatales y supranacionales, la preocupación del empleo de las tecnologías de la información y la comunicación para la comisión de estos hechos delictivos graves.

7. Una arista de regulación trascendente que plantea la Convención de Budapest es lo atinente a la responsabilidad de las personas jurídicas por la comisión de los

delitos informáticos. Así, en su artículo 12, se prevé una serie de criterios normativos de imputación penal contra las personas jurídicas.

Conviene resaltar que, en el sistema penal peruano, ni la Ley n.º 30424 (Ley que regula la responsabilidad administrativa de las personas jurídicas por el delito de cohecho activo transnacional) ni el Decreto Legislativo n.º 1352 (Decreto legislativo que amplía responsabilidad administrativa de las personas jurídicas), así como tampoco el Reglamento de la Ley n.º 30424, prevén la posibilidad de sancionar a la persona jurídica por delitos enmarcados en la ciberdelincuencia. Advirtiéndose como menester la realización de reformas a dichos dispositivos legales, para guardar armonía con los lineamientos normativos internacionales.

8. En lo concerniente a las instituciones procesales que regula el Convenio de Budapest, debemos indicar que este prevé una serie mecanismos y figuras que buscan dotar de efectividad la indagación y acreditación de los delitos enmarcados en la ciberdelincuencia. Así, tenemos que en el artículo 14 del instrumento internacional se hace alusión a la consecución de la «prueba electrónica», en la Ley n.º 30096, no se hace mención ni existe precepto normativo alguno sobre esta institución probatoria.

Por otro lado, debemos destacar que en el artículo 21 del precitado convenio se establecen algunos parámetros normativos sobre la **interceptación de datos relativos al contenido de comunicaciones**; siendo que, respecto a las medidas de obtención y receptación de datos informáticos de comunicaciones específicas con fines de indagación y acreditación de los ciberdelitos, se perciben sus correlatos normativos en la Décima y Undécima Disposición Complementaria Final de la Ley n.º 30096.

Sin embargo, en lo atinente a la **medida de intervención de las comunicaciones**, prevista en el artículo 230 del Código Procesal Penal peruano, la que se habilita para los delitos que posean una pena privativa de liberad superior a los 4 años, se aprecia que en los ciberdelitos previstos en el artículo 2 **(acceso ilícito)** y 10 **(abuso de mecanismos y dispositivos informáticos**) de la Ley n.º 30096 no resultaría viable la aplicación de esta medida, toda vez que su pena privativa de libertad conminada es de máximo 4 años; debiéndose reflexionar sobre algunas propuestas de lege ferenda que dosifiquen el margen de pena abstracto para habilitar tal medida o se eleve el margen punitivo de los referidos ilícitos penales.

Ars Iuris Salmanticensis,
vol. 8, Diciembre 2020, 21-25
eISSN: 2340-5155
Ediciones Universidad de Salamanca - CC BY-NC-ND