Lumen
Ene - Jun. 2020.Vol 16 N°1: pp. 93-100
Doi: 10.33539/lumen.2020.v16n1.2287

CIBERDELINCUENCIA EN TIEMPOS DE COVID-19: ¿LA VULNERACIÓN A DERECHOS CONSTITUCIONALES?

CYBER CRIME IN TIMES OF COVID-19: VIOLATION OF CONSTITUTIONAL RIGHTS?

Fernando Vicente Núñez Pérez*
Brendalis Carhuancho Zaldaña**

* Abogado por la Universidad de San Martín de Porres; Master Internacional en Prevención y Represión del Blanqueo de Dinero, Fraude Fiscal y Compliance por la Universidad de Santiago de Compostela (España); Magíster en Derecho Constitucional y Derechos Humanos por la Universidad Nacional Mayor de San Marcos; Magíster en Ciencias Penales por la Universidad de San Martín de Porres; Miembro Integrante de la Asociación Iberoamericana de Derecho Penal Económico y de la Empresa (AIDPEE). Títulos de Especialización en Derecho Penal Económico y Derechos Humanos, Derecho Penal Económico y Teoría del Delito, ambos otorgados por la Universidad de Castilla – La Mancha (España). Docente en la Facultad de Derecho de la Universidad de San Martín de Porres, dictando los siguientes cursos: Temas de Derecho Procesal Penal II y Derecho Penal Económico (Pregrado); Temas de Derecho Procesal Penal I y Temas de Derecho Procesal Penal III (Postgrado).

** Abogada por la Universidad San Martín de Porres. Cursando la Maestría en Cumplimiento Normativo en Derecho Penal por la Universidad de Castilla-La Mancha, Máster Propio Internacional en Prevención y Represión del Blanqueo de Dinero, Fraude Fiscal y Compliance en la Universidad De Santiago de Compostela (España) y Ciencias Penales en la USMP. Realizó el Programa de Especialización en Compliance por la Universidad del Pacífico y el curso de Especialización Avanzada en Derecho Penal y Procesal Penal en la PUCP.

CIBERDELINCUENCIA EN TIEMPOS DE COVID-19: ¿LA VULNERACIÓN A DERECHOS CONSTITUCIONALES?

CYBER CRIME IN TIMES OF COVID-19: VIOLATION OF CONSTITUTIONAL RIGHTS?

Fernando Vicente Núñez Pérez
Brendalis Carhuancho Zaldaña

RESUMEN:
El uso de internet desarrolló una nueva modalidad de configuración de ilícitos, conocido como Cibercriminalidad. En ese sentido, se ha desarrollado instrumentos internacionales y nacionales para evitar impunidad, buscándose sancionar dichas conductas. El contexto de COVID-19, nos demuestra –muchos más- que nuestras actividades dependen de un soporte tecnológico, lo que genera nuevas modalidades de Cibercriminalidad.

PALABRAS CLAVE:
Cibercriminalidad – derechos constitucionales – ciberdelincuentes - ciberseguridad - delitos informáticos – Convenio de Budapest - Phishing - Cartas Nigerianas - Chantajes informáticos.

Abstract:
The use of the Internet developed a new form of illegal configuration, known as Cybercrime. In this sense, international and national instruments have been developed to avoid impunity, seeking to punish such conduct. The context of COVID-19 shows us - much more - that our activities depend on technological support, which generates new forms of Cybercrime.

KEY WORDS:
Cybercrime - Constitutional Rights - Cybercriminals - Cybersecurity - Computer Crime - Budapest Convention - Phishing - Nigerian Letters - Computer Blackmail.

I. INTRODUCCIÓN

Evidentemente, el uso del internet marcó una notable diferencia en nuestra sociedad. Con el transcurso de los años, la mayoría de nuestras actividades están reflejadas en un soporte virtual, dicha dependencia la advertimos -muchas más- en este contexto de COVID-19.

En ese sentido, podemos afirmar que actualmente, por el contexto COVID-19, han surgido diversas modalidades de Cibercriminalidad, que intentaremos mencionar en el presente artículo, haciendo hincapié que la Cibercriminalidad está en constante evolución, obedeciendo a la naturaleza de dichos ilícitos.

Es decir, conforme la sociedad avanza con la tecnología, también se expone a las conductas delictivas, las mismas que han avanzado notablemente, conocidas como ciberdelincuencia. Si bien, existen instrumentos para la lucha contra la ciberdelincuencia, no es menos cierto que las técnicas para la configuración de dichos delitos vienen evolucionando.

II. ASPECTOS GENERALES DE LA CIBERDELINCUENCIA

Debemos comprender que la ciberdelincuencia forma parte de una problemática a nivel mundial -más aún si tenemos en cuenta- que en las dos últimas décadas aumentó el uso de internet para realizar diversas actividades.

Es así, que la ciberdelincuencia opera en un espacio totalmente diferente a lo que usualmente estamos acostumbrados, esto es, en un espacio virtual; por lo cual, dicha característica fomenta la impunidad.

En ese sentido se define la ciberdelincuencia de la siguiente manera:

> Como el conjunto de aquellas acciones cometidas a través de un bien o sistema informático cuya consecuencia final recae en un hecho considerado como ilícito. En otras palabras, se trata de una vertiente del crimen tradicional que utiliza las nuevas tecnologías para extenderse y desarrollarse de manera exponencial. (Mateos, 2013 p.18)

En ese sentido, podemos afirmar que la ciberdelincuencia evolucionará conforme aumenta la cantidad de usuarios, lo que significa que también aumente la cantidad y modalidad de ciberdelincuencia. Conforme vamos indicando, los ciberdelitos se apoyan en la tecnología, situación que determina una evolución constante.

La mayoría de nuestras actividades se desarrollan en la internet superficial, por ejemplo, pagos, correos, búsquedas, entre otras; sin embargo, existe la internet profunda, la misma que opera –entre otras situaciones- para cometer ilícitos.

Es importante mencionar, que la ciberseguridad es el mecanismo idóneo para el desarrollo de análisis y gestión de riesgos relacionados el ciberespacio. En ese sentido, la ciberseguridad busca neutralizar toda aquella amenaza que se desprenda del uso de del ciberespacio. En ese orden de ideas, podemos afirmar que la ciberseguridad mediante el conjunto de actuaciones busca asegurar la información en el ciberespacio.

Conforme estamos señalando, los ataques al ciberespacio han aumentado tanto en cantidad como en procedimiento, siendo que cada vez mucho más sofisticado, siendo que Fernández y Martínez (2018) señalan: “El robo de datos e información, los ataques ransomware y de denegación de servicios el hackeo de dispositivos móviles y sistemas industriales y los ciberataques contra las infraestructuras críticas son ejemplos de ciberamenazas”. (p.100)

III. EVOLUCIÓN INTERNACIONAL DE LA CIBERDELINCUENCIA

3.1. Comité de Europeo para los Problemas Criminales – CDPC

Respecto al Comité de Europeo para los Problemas Criminales, Tenorio (2018) indica:

> En noviembre de 1996 el Comité de Europeo para los Problemas Criminales (CDPC) vía decisión número CDPC/103/211196 establece un “Comité de Expertos Encargados de Delitos Informáticos” para examinar revisar las recomendaciones 89 y 95 sobre procedimiento penal vinculado a la tecnología de la información y elaborar un borrador de instrumentos jurídicamente vinculante.(p. 36)

Se debe precisar que dicho comité sirvió como base para la creación del Comité de Expertos en la Delincuencia en el Ciberespacio.

3.2. Comité de Expertos en la Delincuencia en el Ciberespacio

En 1997, un grupo de expertos se reunieron para debatir los problemas que oscilaban la delincuencia en internet, siendo que luego sirvió para dar luz al Convenio sobre Ciberdelincuencia, también conocido como Convenio de Budapest.

En ese sentido, Tenorio (2018) indica:

> El nuevo comité se encargó de elaborar un borrador del instrumento entre abril de 1997 y diciembre del año 2000 con recomendaciones de expertos y la participación de Estados miembros y no miembros del Consejo de Europa. En abril del 2000 se desclasificó y publicó el proyecto de Convenio que seguiría siendo modificado en los siguientes meses. (p. 36-37)

3.3. El Convenio de Ciberdelincuencia del Consejo de Europa

En noviembre de 2001, en Budapest se firmó el convenio de Ciberdelincuencia del Consejo de Europa, donde –principalmente- se clasificó los delitos informáticos en cuatro grupos, entre ellos, delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; delitos informáticos; delitos relacionados con el contenido y delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Es importante mencionar que dicho Convenio surgió en un contexto de desarrollo tecnológico sobre internet, situación que modificó parte de la economía. Ahora bien, debemos tener en cuenta que la evolución del internet logró cruzar fronteras, lo que genera la globalización, término muy escuchado en los últimos años.

Es así, que Salom (2010) precisa: “Este Convenio pretende armonizar la legislación de los diversos países que lo ratifiquen, no sólo en materia de derecho penal sustantivo, sino también de derecho procesal para hacer frente a este tipo de delincuencia” (p. 136)

En el año 2003, se creó un Protocolo adicional al Convenio, donde se incluyó conductas como apología del racismo y xenofobia mediante internet.

Es importante mencionar que dichos instrumentos internacionales, hacen advertir que la comisión de ilícitos se realiza de modo virtual, considerándose como delitos informáticos.

Podemos concluir, que el Convenio de Budapest es considerado como el máximo referente respecto a la delincuencia informática.

IV. LA VULNERACIÓN DE DERECHOS CONSTITUCIONALES:

El derecho a la intimidad recogido en nuestra Constitución Política del Perú busca proteger el aspecto reservado de la vida de cada persona, vulnerándose datos personales que forman parte de la esfera privada.

En ese orden de ideas, Fernández y Martínez (2018) señalan:

> El reconocimiento del derecho a la intimidad personal y familiar tiene por objeto, garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona, frente a la acción y el conocimiento de los demás, sean estos poderes públicos o simples particulares. (p.137)

Los ciberdelincuentes utilizan información del entorno de nuestra intimidad para realizar la conducta ilícita. Por ejemplo, conocen nuestros datos personales, bancarios, académicos, entre otros. En ese sentido, la información recopilada coadyuva a que el mecanismo empleado no pueda ser advertido por la víctima.

Continuando, respecto al derecho al secreto de las comunicaciones Fernández y Martínez (2018) señalan:

> Por comunicación entiende la doctrina mayoritaria que deben entenderse incluidos todos los medios de comunicación, no existe un numerus clausus respecto de los medios de comunicación que pueden ser objeto de vigilancia; y para que haya comunicación se exige una distancia real entre los comunicantes y que se realice por canal cerrado. (p.141)

Es necesario que los ciberdelincuentes posean toda la información necesaria para realizar la actividad criminal, siendo que para ello deben obtener vulnerar algunos derechos constitucionales, entre ellos, el secreto de las comunicaciones.

Ahora bien, en relación al derecho a la libertad de expresión e información, el mismo que –en el transcurso del tiempo – ha merecido mucho debate, implica –en términos sencillos- que no afecte al derecho a la intimidad, siendo que en el tema en particular, los ciberdelincuentes obtienen la información sin el consentimiento de la víctima y que utilizan dicha información para cometer un ilícito.

V. EVOLUCIÓN NACIONAL DE LA CIBERDELINCUENCIA

El Perú forma parte del Convenio de Budapest, siendo que dicho instrumento internacional busca combatir y erradicar la ciberdelincuencia.

Es importante definir a los delitos informáticos, siendo:

> Se define a los delitos informáticos no como nuevas conductas ilícitas, sino como nuevas formas como se desarrollan los delitos mediante el uso de medios informáticos conectados a Internet o de manera física teniendo acceso a un dispositivo con algún puerto que permita una conexión al sistema y a los archivos que están contenidos. (Tenorio, 2018, p.11)

Entre los principales delitos informáticos, podemos agrupar en delitos contra la intimidad, relativos al contenido, a la piratería, sabotaje y contra la propiedad intelectual. Se debe indicar, que existe conexión entre ciberdelincuencia y delito informático, siendo que no se puede excluir entre un concepto y otro.

Nuestro país, incorporó los delitos informáticos mediante la Ley Nº 30096 que fue promulgada el 22 de octubre de 2013; sin embargo, dicha ley trae consigo modificatorios, conforme se detalla:

5.1. Ley Nº 30096

Fue promulgado el 22 de octubre de 2013. Es pertinente mencionar, que con la promulgación de la Ley Nº 30096 se deroga los artículos incorporados por la Ley Nº 30076. En ese sentido, desde el año 2000 contábamos con una regulación de delitos informáticos, siendo que el 2013 se crea nuevos ilícitos.

Se advierte de la Ley Nº 30096, buscó prevenir la comisión de aquellas conductas ilícitas que tengan como soporte un sistema tecnológico, luchando contra la Cibercriminalidad.

Podemos señalar, que con Ley Nº 30096 se busca proteger diversos bienes jurídicos, teniendo como referencia el Convenio de Budapest.

5.2. Ley Nº 30171

Ley que modificó la Ley Nº 30096, en fecha 10 de marzo 2014, siendo que la finalidad fue complementar lo regulado por la Convención de Budapest.

5.3. Ley Nº 30838

La Ley Nº 30838, promulgada el 04 de agosto de 2018, es considerada como una de las máximas reformas en lo que refiere a delitos sexuales; por ejemplo, entre las agravantes se añade a quien registre como medios audiovisuales el delito o difunda por las redes sociales.

5.4. Ley Nº 30963

Promulgado el 18 de junio de 2019, modifica el Código Penal, Código de Ejecución Penal y Código de los niños y adolescentes, siendo que se modificó el artículo 5º de la Ley 30096.

VI. FORMAS Y MÉTODOS DE CIBERDELINCUENCIA

Existen diversas formas y métodos de ciberdelincuencia, las mismas que surgen constantemente y pueden ser consideradas como actos preparatorios para la configuración de un ilícito penal, pese a ello, describiremos los siguientes:

6.1. Phishing:

Considerado como una modalidad de ciberdelincuencia, siendo que este método es mucho más novedoso y requiere mayor elaboración. Siendo que, Paredes (2013) define:

> La terminología de esta conducta, derivado del verbo fishing (pescar), se refiere al envío de e-mail utilizando el nombre de un banco en el cual se coloca un link y web falsa mediante el cual induce al usuario a dar información confidencial sobre sus cuentas bancarias, tarjeta de crédito o su clave secreta. (p. 73)

El phishing es la suplantación o clonación de determinados sitios web, entre ellos, entidades bancarias. Algunos expertos, sostienen que dicho mecanismo puede ser considerado como una estafa informática.

Actualmente, el correo electrónico suplantó –en su mayoría- el envío de cartas mediante agencias, siendo que las entidades financieras utilizan el mecanismo de correo electrónico, que facilita la concurrencia de ilícitos, ya que esta modalidad usa un correo electrónico, logotipo, link similar a la entidad financiera.

6.2. Cartas Nigerianas:

Es una modalidad de ciberdelincuencia antigua, entendiéndose que es distinto a las actuales modalidades que se caracterizan por ser más novedosos y elaborados.

Así las cosas, Devia (2017) indica:

> Las llamadas cartas nigerianas, consiste en una inesperada comunicación mediante cartas sobre todo a través de correos electrónicos el remitente, promete negocio muy rentable. (p.204)

En términos sencillos, consiste en la recepción de un correo electrónico con información de un usuario desconocido, donde se anuncia información de alguna herencia o datos bancarios, siendo que posteriormente dicha información es usado para ilícitos.

En esta modalidad, el tiempo juega un rol fundamental, ya que solicitan que se responda el correo en un plazo, por ejemplo de un día.

6.3. Chantajes informáticos:

Es una modalidad de ciberdelincuencia muy conocida, consiste en la llamada a familiares indicando que existe una posible víctima de secuestro, donde se solicita el pago de una determinada cantidad de dinero.

Hemos advertido por los medios de comunicación, que esta modalidad es muy usada por los ciberdelincuentes. Ahora bien, en esta modalidad, la organización criminal realiza una actividad previa, esto es, corroborar información.

6.4. Wannacry:

También llamados secuestros informáticos, versa en introducirse en la computadora o el ordenador de la víctima, añadiendo archivos, base de datos o documentos.

El origen de este tipo de ciberdelincuencia es desconocido, aunque algunos expertos sostienen que se solicitaba un rescate mediante bitcoins. Si bien, los documentos o archivos no se dañan, lo que sucede es que se convierten en inaccesibles.

En ese sentido, el Código Penal Español, mediante el artículo 264.1º sostiene: “El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesible datos informáticos”.

6.5. Llamada perdida:

Es una modalidad de ciberdelincuencia mucho más habitual, ya que versa en la recepción en un teléfono móvil desde un número desconocido.

Es preciso advertir que durante la llamada, se advierte que en un buzón de voz se ha dejado un mensaje, siendo que para oír ese mensaje, el usuario se suscribe sin saberlo a un servicio de mensajería, el mismo que permite facturar una determinada cantidad de dinero.

6.6. Sim Swapping:

Es una modalidad de ciberdelincuencia actual, consiste en dejar sin cobertura a los teléfonos móviles y clonar o cancelar la tarjeta SIM.

Conforme hemos precisado, los ciberdelincuentes se apoyan de diversas modalidades para lograr nuevas formas y métodos de ilícitos, los mismos que en su mayoría son más calificados.

Asimismo, en el contexto del COVID-19, donde muchas personas se están apoyando en un soporte tecnológico para diversas actividades, entre ellas, pagos, estudios, trabajo y otros.

VII. CARACTERÍSITICAS DE LA CONDUCTA DE LA CIBERDELINCUENCIA

Conforme hemos señalado, la ciberdelincuencia se caracteriza por desarrollarse en una plataforma virtual, siendo que el sujeto oculta su identidad, situación que genera dificultad para una futura investigación. Por ejemplo, mediante la Deep Web o también conocido como la internet profunda, se busca crear perfiles falsos.

Por lo cual, podemos indicar que existen comportamientos y situaciones particulares, incluso algunas conductas que no son conocidas a la fecha, situación que genera impunidad a la fecha.

Ahora bien, como la ciberdelincuencia se desarrolla en una plataforma virtual, es posible que la configuración de la ciberdelincuencia se desarrolle con la colaboración de diversos sujetos que se encuentren en diferentes Estados. Por lo cual, en la ciberdelincuencia es posible advertir los ataques masivos, lo que significa que existe una organización criminal.

VIII. CONCLUSIONES

- Se recomienda, para evitar ser víctima de la cibercriminalidad, tomar en cuenta los consejos que se proporcionan a los usuarios. Asimismo, tener en cuenta el sentido común y el principio de desconfianza, más aún cuando nos solicitan datos que no son habituales ni comunes.

- La naturaleza de la cibercriminalidad nos hace entender que no conoce frontera; por ello, se necesita de una lucha internacional contra estas organizaciones criminales.

- Es necesario la implementación internacional de un sistema que busque prevenir ciberataques; por ejemplo, en España existe el Centro Nacional de Protección de las Infraestructuras Críticas.

- Nuestra legislación sobre delitos informáticos, propone un catálogo de conductas ilícitas que buscan evitar impunidad.

- Además, es necesario implementar una política criminal global, que busque evitar impunidad, esto es, frente a problemas globales se necesita de soluciones de características similares.

IX. REFERENCIAS BIBLIOGRÁFICAS

- Devia, E. (2017). *Delito informático: Estafa informática del artículo 248.2 del Código Penal.* Tesis para obtener el grado de Doctor en la Universidad de Sevilla. Disponible en: https://idus.us.es/bitstream/handle/11441/75625/Tesis%20Edmundo%20Devia%20Completa%20Final%2031%20Mayo%202017.pdf?sequence=1&isAllowed=y, confrontado con fecha 22 de julio de 2020.
- Fernández, D. y Martínez, G. (2018). *Ciberseguridad, ciberespacio y ciberdelincuencia.* Thomson Reuters Aranzadi.
- Mateo, I. (2013). *Ciberdelincuencia, desarrollo y persecución tecnológica.* Universidad Politécnica de Madrid. Disponible en: http://oa.upm.es/22176/1/PFC_IVAN_MATEOS_PASCUAL.pdf, confrontado con fecha 15 de junio de 2020.
- Paredes, J. (2013). *De los delitos cometidos con el uso de sistemas informáticos en el distrito judicial de Lima, en el período 2009-2010.* Tesis para obtener el grado de Magister en Derecho con mención en Ciencias Penales en la Universidad Nacional Mayor de San Marcos. Disponible en: https://hdl.handle.net/20.500.12672/10314 , confrontado con fecha 19 de junio de 2020.
- Tenorio, J. (2018). *Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia.* Academia Diplomática del Perú “Javier Pérez de Cuéllar”. Disponible en: http://repositorio.adp.edu.pe/handle/ADP/71 , confrontado con fecha 26 de junio de 2020.

Fecha de recepción: 22 de mayo de 2020
Fecha de aceptación: 01 de junio de 2020