El hack-back como modalidad de legítima ciberdefensa

Jacobo Alejandro González Cortés[1]

El numeral 6 del artículo 32 del Código Penal Colombiano tiene consagrada la figura de la legítima defensa como causal de justificación. Esta institución opera cuando exista la necesidad de defender un derecho propio o ajeno contra injusta agresión actual o inminente. A su turno, la multiplicidad de ataques informáticos ha hecho que cada día existan más y más empresas especializadas en ciberseguridad. De ahí que nos preguntemos: ¿la causal referida puede adaptarse al hack-back? Existen diferentes teorías al respecto, cuya aplicabilidad será analizada dentro del tema concreto.

Sumario:

I. Introducción

En el año 2017, el mundo fue objeto de un gran ciberataque hecho por el programa malicioso denominado ***WannaCry***. Esto generó una alerta para las grandes potencias a nivel mundial, las cuales, inmediatamente, reaccionaron para buscar mecanismos que permitieran combatir estas

[1] Abogado de la Universidad Militar Nueva Granada. Candidato a Magíster en Derecho con énfasis en Procesal Penal de la Universidad Sergio Arboleda. Ha sido ponente en congresos de delitos informáticos y participó en el Primer simposio nacional de delitos informáticos, en el que se abordaron aspectos de técnicas de investigación, entre otros. Ha capacitado, a nivel nacional, a fiscales, miembros del CTI y de la Policía Judicial. Actualmente, es socio de la firma MPa abogados y se desempeña como director de operaciones por sus amplios conocimientos en el manejo de delitos informáticos y financieros, así como de las facultades de las víctimas en el proceso penal. Ha ocupado diversas posiciones en la firma en más de una década de trabajo.

agresiones digitales masivas. Producto de esta situación, se generó una técnica de defensa denominada *hack-back,* que significa, en palabras sencillas, devolver el ataque, una especie de legítima ciberdefensa, la cual, como veremos adelante, puede ser aplicable en la legislación colombiana.

Para lograr lo anterior, hablaremos del origen del *hack-back* y tocaremos, someramente, cómo la Unión Europea, la OTAN y el Senado de los Estados Unidos de América han venido creando, desde sus perspectivas, una legislación para el uso de esta técnica de defensa. Se verificará cómo en Colombia nuestra legislación puede permitir, bajo el criterio de la legítima defensa, el devolver el ataque y, finalmente, estableceremos los parámetros que deben cumplirse al momento de realizar una actividad de legítima ciberdefensa de cara a la delincuencia informática.

II. El origen del hack-back como mecanismo de legítima ciberdefensa

El mundo digital ha obligado a los entes corporativos a permanecer conectados a la red so pena de perder vigencia. Se estima que casi el 90% de los activos corporativos son digitales[2] y la mayor fuente de información se encuentra en el ciberespacio, así como la mayor cantidad de clientes y usuarios. Es por esto que, por ejemplo, todas las entidades financieras le están apostando a la digitalización de los productos. El sector real ve en los sistemas informáticos un gran aliado para el desarrollo comercial de sus empresas; los comerciantes hacen un gran porcentaje de sus negocios a través de la red, y son las plataformas electrónicas los vehículos de éxito para muchos negocios.

Pero, así como esta era digital ha traído grandes beneficios, también existen grandes preocupaciones y riesgos. La ciberdelincuencia ha crecido protuberantemente[3]; diferentes

2 ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA) e INTERNET SECURITY ALLIANCE. Manual de supervisión de riesgos cibernéticos para juntas corporativas, 2017.

3 “Amenazas cibernéticas en cifras

• Estimar el daño de los ataques cibernéticos es difícil, pero algunos lo estiman en $ 400-500 mil millones o más anualmente, en la que no se detecta una parte significativa de los costos. Los costos de la ciberdelincuencia se quintuplicaron entre 2013 y 2015 y podrían alcanzar los $ 2 billones por año para 2019.

• La ciberseguridad se encuentra entre los principales riesgos para los mercados de América Latina, según una encuesta de profesionales que trabajan, o no, en el campo de riesgos.

modalidades de ataques informáticos, como el *ransomware*[4], el *phishing*[5], el *smishing*[6]**,** el DDoS[7], la ingeniería social, entre otros, están a la orden del día. Recordamos el año 2017, cuando el mundo fue objeto de un gran ciberataque hecho por el malware denominado ***WannaCry*** (en inglés ***WannaCry ransomware attack*** *o* ***WannaCry Doble Pulsar Attack***)[8]. Este ataque, que estaba dirigido a entes con estructuras críticas[9], a grandes empresas del sector real, gubernamental e, incluso, del sector de la salud, se volvió masivo en el mundo entero.

Colombia[10] tampoco estuvo a salvo, toda vez que, al Hospital Carlos Holmes Trujillo de Cali, le fue secuestrada su información a cambio de una recompensa que debía ser cancelada con

---

• Brasil, Argentina y México ocupan el tercer, octavo y décimo lugar, respectivamente, en los rankings globales de países de origen para los ciberataques.

• Los ataques de ransomware en América Latina aumentaron un 131% en el último año México y Brasil ocupan el séptimo y octavo lugar en el mundo por ocurrencia de la mayoría de los ataques de ransomware.

• El 34% de todo el fraude por originación (sic) de nuevas cuentas proviene de América del Sur.

• El 80 por ciento de los ciberataques se deben al crimen organizado.

• La mediana de días transcurridos entre el momento en que una organización está comprometida y que se descubre la violación cibernética es 14619. El 53 por ciento de los ataques cibernéticos son identificados primero por terceros (por ejemplo, agentes de la ley o socios corporativos), y solo el 47 por ciento se descubre internamente

• El 48 por ciento de los profesionales de seguridad de TI no inspeccionan la nube en busca de malware, a pesar del hecho de que el 49 por ciento de todas las aplicaciones empresariales ahora están almacenadas en la nube. De esas aplicaciones basadas en la nube, el departamento de TI conoce, sanciona o aprueba menos de la mitad.

• "El 38 por ciento de las organizaciones de TI no tienen un proceso definido para revisar sus planes de respuesta a la violación cibernética, y casi un tercio no ha revisado ni actualizado sus planes desde su desarrollo inicial". Extracto del "Manual de supervisión de riesgos cibernéticos para juntas corporativas", 2017, pp. 9 y 10.

4 Modalidad delictiva en la que se realiza el secuestro de información de un ordenador o de un dispositivo especifico, mediante el cual el delincuente solicita un beneficio para el rescate de la información".

5 Modalidad delictiva en la que el delincuente informático, a través de sitios web ficticios o medios semejantes, capturan los datos de las personas para dar un uso, por lo general ilegítimo.

6 Es la misma modalidad anterior, pero la forma de engañar al usuario víctima es a través de mensajes de texto.

7 Es una modalidad delictiva, considerada como una modalidad de denegación del servicio que proviene del inglés "distributed denial of service" y, en palabras comprensibles, congestionan la capacidad de respuesta de un programa o servicio, para sacarlo del mercado temporalmente.

8 WIKIPEDIA. Ataques ransomware WannaCry. En: WIKIPEDIA. [sitio web], 29 mayo 2020. [Consultado el 1 de junio de 2021] Disponible en: https://es.wikipedia.org/wiki/Ataques_ransomware_WannaCry

9 "Las infraestructuras críticas son aquellas sin las que una sociedad no puede mantener el ritmo de vida que ha mantenido con anterioridad. Son las que se mantienen, protegen y supervisan con márgenes de seguridad amplios para que siempre se pueda contrarrestar cualquier tipo de situación complicada. Siempre son estructuras que están sobreprotegidas, dado que nunca se debe llegar a la situación de que se produzca un incidente grave en ellas. Las estructuras críticas incluyen las redes gubernamentales, los equipos físicos de suma importancia, los sistemas de almacenamiento que estén centralizados con todos los datos de los ciudadanos y los servicios fundamentales para la vida, como la electricidad o el gas. Las administraciones públicas, las distintas instituciones gestionadas por el estado (sic) y otros elementos similares quedan también dentro de este grupo". UNIVERSIDAD INTERNACIONAL DE VALENCIA. ¿Qué se considera una infraestructura crítica? [En línea] 21 de marzo de 2018. Disponible en: https://www.universidadviu.com/se-considera-una-infraestructura-critica/

10 EL ESPECTADOR. Así llegó WannaCry a Colombia. EL ESPECTADOR. [en línea]. 17, mayo, 2017. [Consultado el 1 de junio de 2021]. Disponible en: https://www.elespectador.com/noticias/judicial/asi-llego-wannacry-colombia-articulo-694262

criptomonedas conocidas como "*bitcoins*"[11]. Fue un ataque sin precedentes: 150 países afectados y más de 230.000 computadoras infectadas. Sólo un hacker anónimo, denominado *"Malware tech",* logró desactivar el virus. Ni los entes gubernamentales, ni las agencias especiales pudieron impedirlo.

Este hecho y las posibilidades que tenían los ciberdelincuentes de hacer ataques masivos, como el relatado, que, en cuestión de horas, afectó a un importante número de computadores y sistemas de información, suscitó una sesión en Bruselas, el 13 de septiembre de 2017[12], promovida por la Unión Europea, en conjunto con la OTAN[13], en la que se creó una comisión para dar respuesta a los ciberataques. Por su parte, en los Estados Unidos de América, el representante Tom Graves presentó al Senado un proyecto de ley titulado "Ley de seguridad activa de la defensa cibernética", el cual no tuvo acogida. Este mismo proyecto se volvió a presentar el 11 de junio de 2019[14], esta vez de manera conjunta por el representante Josh Gottheimer y su primer promotor, Graves.

Hay una diferencia entre lo que plantea la UE y los representantes de los EE.UU. En efecto, la UE ha pensado en la implementación de una ciberdefensa para temas de seguridad nacional, inteligencia, contrainteligencia y/o prevención del terrorismo; están en la discusión de extender estas figuras a algunos entes corporativos de infraestructuras críticas que puedan ser objeto de ataque. Entre tanto, en el proyecto de ley que cursa en los Estados Unidos, se habla de la utilización de la ciberdefensa, no solo para la defensa del Estado, sino, incluso, para los particulares. Esto llama la atención, ya que el proyecto contempla procedimientos de utilización de fuerza en los que se devuelve el ataque al ciberdelincuente, lo que podría convertirse en un "ciberoeste", y afectar el buen comportamiento del ciberespacio. La discusión está sobre la mesa y serán los debates los que permitirán delimitar esta modalidad defensiva.

---

11 ANTROPOULOS, Andreas. Mastering Bitcoin. Unlocking Digital Crytocurrencies. Sebastopol: O' Reilly, 2015. p. 61 "Bitcoin es un monedero electrónico compuesto por cadena de firmas diales, en líneas resumidas en un sistema de pago electrónico basado en la prueba criptográfica. Las técnicas criptográficas se utilizan en él para proveerle seguridad a las transacciones y mantener el libro de contabilidad distribuido".

12 "El 13 de septiembre, en su discurso anual sobre el estado de la Unión, el presidente Jean-Claude Juncker declaró: "En los últimos tres años, hemos avanzado para mantener a los europeos seguros en línea. Pero Europa todavía no está bien equipada cuando se trata de ciber- ataques. Por eso, hoy, la Comisión propone nuevas herramientas, incluida una Agencia Europea de Ciberseguridad, para ayudarnos a defendernos de tales ataques". THE ECONOMY JOURNAL. La Comisión Europea amplía la respuesta de la UE a los ciberataques. [En línea]. 17, octubre, 2020. [Consultado el 17 de octubre de 2020] Disponible en: https://www.theeconomyjournal.com/texto-diario/mostrar/941919/comision-europea-amplia-respuesta-ue-ciberataques.

13 La Organización del Tratado del Atlántico Norte, también denominada la Alianza Atlántica, es una alianza militar intergubernamental que se rige por el Tratado del Atlántico Norte o Tratado de Washington, firmado el 4 de abril de 1949.

14 CLERK. UNITED STATES HOUSE OF REPRESENTATIVES. Inicio [sitio web]. Washington D.C. [Consultado el 17 de octubre de 2020]. Disponible en: https://tomgraves.house.gov/uploadedfiles/gravga_007_xml.pdf

A pesar de la diferencia, y en esto coinciden quienes se han interesado por estas temáticas (UE, OTAN, EE.UU.), se puede implementar dentro de las actividades de la seguridad de la información y la ciberdefensa la modalidad de *hack-back.*

El *hack-back*, no es otra cosa que devolver el *hackeo* o utilizar la fuerza para repeler el ataque. Se puede hacer de manera reactiva, en el momento en que alguien (sea persona jurídica o natural) esté siendo víctima de un ciberdelito, o, también, de manera preventiva para disuadir la actividad delictiva ante una amenaza que sea real. Sin embargo, del segundo caso no nos ocuparemos en esta columna, dado que se dificulta sustentarla jurídicamente en la legítima defensa. Precisamente, la forma en que se diseña la modalidad de defensa contra los ciberataques es la que provoca la reflexión de esta columna. En efecto, es válido preguntarse si el ordenamiento jurídico colombiano podría permitirlo, pues, teniendo en cuenta la figura de la legítima defensa, suena razonable que se tomen medidas de esta naturaleza, de manera reactiva, para contrarrestar este tipo de ataques, mas no de manera preventiva, cuando la sospecha puede o no resultar razonable.

A diario, se libran ciberbatallas para impedir los ataques informáticos, pero realmente no existen unos parámetros claros de cómo realizar la actividad de ciberdefensa. De ahí que se plantean varios interrogantes: ¿cuándo se puede entender que la acción es ilegítima por parte del cibernauta?, ¿en qué momento se considera inminente un ciberataque?, ¿hasta qué punto puede realizarse la actividad de devolver el *hackeo*?, ¿cómo puede entenderse la proporcionalidad en el mundo cibernético? y ¿qué pasa si estamos ante una actividad que surge de la provocación? En lo que sigue, intentaremos resolver estas y otras dudas que suscita la figura en comento.

III. *Hack-back* como legítima defensa en el ordenamiento jurídico colombiano

De acuerdo con nuestro ordenamiento jurídico, existe la figura de la legítima defensa, contemplada en el Código Penal, en su artículo 32[15]. En palabras simples y menos técnicas, la legítima defensa

15 COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 599. (24, julio, 2000). Por la cual se expide el Código Penal. Diario oficial. Julio, 2000. No. 44097. "ARTICULO 32. AUSENCIA DE RESPONSABILIDAD. No habrá lugar a responsabilidad penal cuando: numeral 6. Se obre por la necesidad de defender un derecho propio o ajeno contra injusta agresión actual o inminente, siempre que la defensa sea proporcionada a la agresión".

opera cuando se permite a un ciudadano defenderse a sí mismo o a un tercero de una agresión grave e injusta por parte de alguien que pretenda causar daño o cometer una actividad de relevancia penal.

La Corte Suprema de Justicia ha fijado los requisitos que deben confluir[16] para poder hablar de legítima defensa, criterios que han sido reiterados en varias oportunidades por esta corporación[17]; sin embargo, para el tema que nos ocupa, aun cuando parece bastante sencilla su adaptación y comprensión para casos comunes, en el tema de los ciberataques, no lo es. Por esto, es necesario considerar los criterios mínimos que deben ser tenidos en cuenta para implementar una técnica de legítima defensa como el *hack-back*, conforme a los lineamientos de la Corte Suprema de Justicia.

Vale aclarar que no todas las modalidades de *"hack–back"* pueden ser usadas. Por ejemplo, aquella que se realice sin una amenaza actual o inminente, o la actividad derivada de una simple sospecha. Un ejemplo claro de esta situación es aquel en que la modalidad de *hack-back* se utiliza como mecanismo de disuasión ofensiva adicional a las actividades de seguridad preventiva.

La base fundamental para implementar una legítima ciberdefensa es que el ciberataque esté sucediendo en el momento mismo o instantes previos al que se aplica el *hack-back*. Esta temporalidad en el hecho es de bastante importancia para determinar la legitimidad de la modalidad de defensa. Bien lo dijo la Corte Suprema de Justicia en su Sala Penal: "Surge patente que en la eximente de responsabilidad en comento la necesidad de la defensa está determinada por la existencia previa o concomitante de una agresión, entendida ésta, en sentido lato, como la conducta

16 COLOMBIA. CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN PENAL. Sentencia SP1784-42440. (15, mayo, 2019). M.P.: Eugenio Fernández Carlier. "La legítima defensa es el derecho que la ley confiere de obrar en orden a proteger un bien jurídicamente tutelado, propio o ajeno, ante el riesgo en que ha sido puesto por causa de una agresión antijurídica, actual o inminente, de otro, no conjurable racionalmente por vía distinta, siempre que el medio empleado sea proporcional a la agresión. Requiere, por tanto, para su configuración, que en el proceso se encuentre acreditado la concurrencia de los siguientes elementos: a). Que haya una agresión ilegítima, es decir, una acción antijurídica e intencional, de puesta en peligro de algún bien jurídico individual [patrimonio económico, vida, integridad física, libertad personal]. b). Que sea actual o inminente. Es decir, que el ataque al bien jurídico se haya iniciado o inequívocamente vaya a comenzar y que aún haya posibilidad de protegerlo. c). Que la defensa resulte necesaria para impedir que el ataque injusto se materialice. d) Que la entidad de la defensa sea proporcionada, tanto en especie de bienes y medios, como en medida, a la de la agresión. e) Que la agresión no haya sido intencional y suficientemente provocada. Es decir que, de darse la provocación, ésta no constituya una verdadera agresión ilegítima que justifique la reacción defensiva del provocado".

17 COLOMBIA. CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN PENAL. Providencia AP1018-43033. (5, marzo, 2014). M.P.: Fernando Alberto Castro Caballero; COLOMBIA. CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN PENAL. Expediente 32598. (6, diciembre, 2012). M.P.: Julio Enrique Socha Salamanca; COLOMBIA. CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN PENAL. Sentencia SP2192-38635. (4, marzo, 2015). M.P.: Eugenio Fernández Carlier.

intencional de otro orientada a producir daño a un bien jurídico, o en términos legos, como el acto, de acometer a alguien para matarlo, herirlo o hacerle daño"[18].

Es decir, debe existir una agresión al bien jurídico o ser inminente su materialización. En este caso, se hace referencia a cualquier delito que pueda ser cometido a través de la red (sin enfocarnos, únicamente, en los delitos informáticos, toda vez que, precisamente, se trata de combatir la ciberdelincuencia como tal). Además, la persona que actúa debe tener la capacidad de repeler el ataque y devolverlo, o llevar a cabo actividades viables para impedirlo. Esto aplica, por lo general, a un ingeniero o un técnico experto en seguridad de la información o en *hacking* ético.

Adicional a lo anterior, frente al tema de la temporalidad del hecho provocador del *hack-back*, es preciso aclarar que, en algunos casos, resulta de mucha dificultad la identificación del momento en que ocurrió el delito. Por lo anterior, y dado que la modalidad de legítima ciberdefensa *hack-back* no puede ser usada de manera post delictual, será un desafío para los expertos el determinar la actualidad de la agresión.

En principio, en los casos en los que el ciberataque sea de ejecución permanente, como el secuestro de información, que puede adecuarse típicamente a un constreñimiento ilegal, las condiciones persisten y no hay problema como tal. Pero, en casos como el *phishing,* que, por lo general, encuadra en el delito de violación de datos personales, por el verbo rector de "compilar", donde la obtención de los datos ya pudo haber sucedido, es dudosa la forma en que se plantea la inminencia del ataque. Por el contrario, podría hablarse de una especie de "venganza privada" al momento de aplicar actividades de *hack-back*. Estos casos no son considerados como una causal de justificación por parte de la ley en Colombia.

También, se debe tener en cuenta, en materia de ciberdelincuencia, que pueden existir muchas formas de impedir el ataque mediante herramientas tecnológicas de protección ante vulnerabilidades de los sistemas; son aquellas que, simplemente, bloquean el programa malicioso, tales como los cortafuegos o *firewalls*. Por ello, ante la necesidad de repeler el ciberataque, no siempre se debe recurrir al *hack-back,* pues existen otros mecanismos para hacerlo (*firewall*, parche, políticas de seguridad anti-intrusivas), que son menos invasivos. Por lo tanto, en la legítima ciberdefensa, el

18 COLOMBIA. CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN PENAL. Providencia AP1018-43033. (5, marzo, 2014). M.P.: Fernando Alberto Castro Caballero.

hack-back resulta necesario para impedir que el ataque injusto se materialice, pero, si hay una forma menos invasiva, es necesario recurrir primero a ella.

En relación con la proporcionalidad del ataque, es más difícil de determinar, pues la cuestión es netamente técnica. Es fundamental, para el operador técnico o profesional, determinar que el uso de la ciberfuerza resulte acorde con el ataque, pues, en el escenario de una persona que pretende acceder a un sistema informático, combinando claves posibles mediante procesos mecánicos, no puede realizarse un contra *hackeo* que acceda a su sistema informático, borre todos los archivos de su dispositivo electrónico e inhabilite su computador.

Otra indicación por seguir es que, en ninguna circunstancia, debe generarse un escenario de provocación al agresor que pueda resultar en una ciberdefensa a través del *hack-back.* Ha habido casos, por ejemplo, en que un técnico incita al delincuente para que emprenda un ciberataque y, atendiendo el cambio de actitud generado por la provocación del técnico, este último emprende una actividad de devolución del *hackeo* amparado en una legítima defensa.

En estos términos, existe la viabilidad de realizar una legítima ciberdefensa a través de la modalidad de *hack-back*. Lo claro es que estos procesos implican conocimientos especializados; no cualquiera puede realizarlos y, sobre todo, ante la ausencia de regulación en la materia, resulta prudente buscar fuentes auxiliares, como los criterios internacionales que se han construido en materia de ciberseguridad para no generar desbordamientos en la técnica *hack-back.*

IV. Reflexión final

Si bien es cierto la legítima defensa es válida en nuestro ordenamiento jurídico y esta institución puede ser aplicable para temas de *hack-back,* resulta prudente darle un alcance legal adicional en situaciones de ciberdelincuencia, dadas las complejidades técnicas que puede contemplar, así como se viene haciendo en la UE y en los EE.UU.

Es evidente la falta de regulación en la materia en Colombia, por lo que el llamado será a nuestros legisladores para que, como lo está haciendo la Unión Europea y algunos representantes en el Senado estadounidense, comiencen a explorar la necesidad de regularizar temas de legítima

ciberdefensa. Efectivamente, en un mundo globalizado, en donde, evidentemente, existen riesgos como los que ya fueron expuestos, resulta prudente encontrar mecanismos que sean viables para dar respuesta efectiva a la problemática.

En segundo lugar, el *hack-back* es una actividad poco conocida, pero que hace parte de los servicios de muchas empresas destinadas a la seguridad de la información y a la protección de los sistemas informáticos. Aunque su uso resulta bastante complejo, es una realidad que debe ser implementada para poder afrontar eventos como el *WannaCry*, que, en su momento, afectó en gran medida a muchas entidades y fue lo que, precisamente, motivó la técnica mencionada a lo largo de este escrito.

Finalmente, debemos ser responsables en el manejo de nuestra información y nuestros sistemas informáticos, lo que implica la implementación de mecanismos de auto tutela, de manera que no sea necesario utilizar técnicas tan delicadas como el *hack-back* para repeler un ataque. Por lo tanto, las compañías deben promover campañas de seguridad de información, en las que se sensibilice a los empleados sobre los riesgos asociados a los sistemas informáticos, se implementen políticas claras de seguridad de la información y se utilicen parches, antivirus o cortafuegos, para disminuir los riesgos de los ciberataques.

Bibliografía

ANTROPOULOS, Andreas. Mastering Bitcoin. Unlocking Digital Crytocurrencies. Sebastopol: O' Reilly, 2015.

CLERK. UNITED STATES HOUSE OF REPRESENTATIVES. Inicio [sitio web]. Washington, DC. [Consultado el 17 de octubre de 2020]. Disponible en: https://tomgraves.house.gov/uploadedfiles/gravga_007_xml.pdf

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 599. (24, julio, 2000). Por la cual se expide el Código Penal. Diario oficial. Julio, 2000. Nro. 44097.

COLOMBIA. CONGRESO DE LA REPÚBLICA, Ley 1621. (17, abril, 2013). Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones. Diario oficial. Abril, 2013. Nro. 48.764.

COLOMBIA. CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN PENAL. Expediente 32598. (6, diciembre, 2012). M.P.: Julio Enrique Socha Salamanca.

COLOMBIA. CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN PENAL. Providencia AP1018-43033. (5, marzo, 2014). M.P.: Fernando Alberto Castro Caballero.

COLOMBIA. CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN PENAL. Sentencia SP2192-38635. (4, marzo, 2015). M.P.: Eugenio Fernández Carlier.

COLOMBIA. CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN PENAL. Sentencia SP1784-42440. (15, mayo, 2019). M.P.: Eugenio Fernández Carlier.

EL ESPECTADOR. Así llegó WannaCry a Colombia. EL ESPECTADOR. [en línea]. 17, mayo, 2017. [Consultado el 1 de junio de 2021]. Disponible en: https://www.elespectador.com/noticias/judicial/asi-llego-wannacry-colombia-articulo-694262

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA) e INTERNET SECURITY ALLIANCE. Manual de supervisión de riesgos cibernéticos para juntas corporativas, 2017.

THE ECONOMY JOURNAL. La Comisión Europea amplía la respuesta de la UE a los ciberataques. [En línea]. 17, octubre, 2020. [Consultado el 17 de octubre de 2020] Disponible en: https://www.theeconomyjournal.com/texto-diario/mostrar/941919/comision-europea-amplia-respuesta-ue-ciberataques.

UNIVERSIDAD INTERNACIONAL DE VALENCIA. ¿Qué se considera una infraestructura crítica? [En línea] 21 de marzo de 2018. Disponible en: https://www.universidadviu.com/se-considera-una-infraestructura-critica/

WIKIPEDIA. Ataques ransomware WannaCry. En: WIKIPEDIA. [sitio web], 29 mayo 2020. [Consultado el 1 de junio de 2021] Disponible en: https://es.wikipedia.org/wiki/Ataques_ransomware_WannaCry