La utilización de software como herramienta de interceptación de comunicaciones*

*Cristian Cobo Jiménez***

Resumen: Este artículo efectúa un estudio sobre la legalidad de la utilización de *software* como herramienta de vigilancia de comunicaciones; para llevar a cabo ello, se estudian los nuevos programas de interceptación conocidos como *software* de interceptación, programa malicioso o *software* espía. Estos son cuestionados por la falta de una ley clara que permita su utilización por parte de algunas autoridades del Estado que cumplen funciones en materia de investigación judicial e inteligencia. Asimismo, se analizan mecanismos en derecho para la utilización legal de dicho *software*, las voces en contra de su uso y por qué las autoridades están en desventaja respecto a la obtención de la información si se tienen en cuenta las nuevas formas de comunicación empleadas por la delincuencia organizada.

Palabras claves: Interceptación de comunicaciones, *software*, programa malicioso, mensaje de datos.

Abstract: This article studies the legality of using the software as a tool for communications surveillance, studying the new interception programs known as interception software, malware, or spyware. These are questioned due to the lack of a clear law that allows their use by some State authorities that perform judicial investigation and intelligence functions. It also analyzes mechanisms in law for the legal use of such software, the voices against its use, and why the authorities are at a disadvantage concerning obtaining information, taking into account the new forms of communication used by organized crime.

Keywords: Interception of communications, software, malware, data message.

---

* Artículo de reflexión presentado como trabajo de grado para optar al título de magíster en Derecho, Universidad Sergio Arboleda, Santa Marta (Colombia), dirigido por el profesor Andrés Guzmán Caballero.

** Abogado; especialista en Derecho Penal; magíster en Derecho, de la Universidad Sergio Arboleda. Investigador del Cuerpo Técnico de Investigación de la Fiscalía General de la Nación. Correo de contacto: crisco2014@outlook.es

Introducción

El presente trabajo tiene como finalidad destacar la importancia de la interceptación de llamadas efectuadas por sistemas distintos a la telefonía ordinaria, mediante la utilización de *software* sobre todo cuando se piensa en las actividades de persecución penal; además, pretende analizar si se requieren nuevas formas legales para el control, alcance y su utilización como mecanismo de interceptación de comunicaciones en nuestro medio. Con base en lo anterior se partió de la hipótesis de que, en la actualidad, las autoridades pierden terreno cuando acuden a la interceptación de las comunicaciones en desarrollo de sus tareas investigativas.

En efecto, los entes investigativos no tienen conocimiento de los miles de mensajes y llamadas realizadas a diario a través de diferentes aplicaciones por parte de organizaciones delictivas, lo que es producto de la carencia de herramientas para hacerlo y del abandono de la tradicional llamada telefónica. Sin embargo, los Estados tienen la necesidad de combatir esas formas de criminalidad, máxime si ellas se adaptan a los nuevos medios tecnológicos. Por este motivo, a título de cuestión que resume el problema de investigación, se pregunta: ¿Es necesario el empleo de nuevas herramientas de interceptación para sistemas de datos?

La justificación de la presente investigación radica en que los tiempos cambian y no se puede soslayar que muten las formas de comunicación de las personas, entre las cuales se incluyen las que integran las redes criminales; por ello, se analizan los vacíos legales existentes confrontándolos con la legislación que regula la materia. Asimismo, se recalca la conveniencia de hacer una incursión académica como esta de cara a mejorar el ordenamiento jurídico y aportar a la sociedad en general, en pro de concebir mejores herramientas en la lucha contra la delincuencia que debe enfrentarse con las herramientas legales necesarias y adecuadas.

El objetivo principal, que a la vez se torna en el aporte del trabajo, radica en proyectar la forma en la cual se pueden escuchar las llamadas, por métodos distintos a la telefonía ordinaria e interceptar mensajes de datos, ambas

acciones de manera legal. Como se mencionó, es innegable la velocidad con la cual avanza la tecnología y con ésta se especializa cada vez más el actuar delictivo de los que optan por ese camino; por ende, es relevante la utilización de nuevas herramientas de interceptación de comunicaciones para lograr una efectividad por parte de los entes investigativos.

Para cumplir con este objetivo, el trabajo se estructura en tres capítulos: en el primero, se esboza el contenido histórico, literal y normativo de la interceptación de comunicaciones; en el segundo, se muestra al *software* como una herramienta de interceptación de mensajes de datos; y, en el tercero, se efectúa un breve recorrido por el derecho comparado frente al uso de esta herramienta tecnológica, a partir de tres ordenamientos específicos. Al final, se incluyen las conclusiones y se abre un espacio para el debate académico sobre las nuevas herramientas de interceptación de comunicaciones en nuestro medio.

La interceptación de comunicaciones

Breves apuntes sobre la interceptación de comunicaciones.

Desde el punto de vista literal, se entiende por interceptar: "1. tr. Apoderarse de algo antes de que llegue a su destino. 2. tr. Detener algo en su camino. 3. tr. Interrumpir, obstruir una vía de comunicación" (RAE, 2019, párr. 1). A su turno, según Leal (2011) para que exista comunicación deben concurrir como mínimo dos personas intercambiando mensajes, debe existir un emisor, un receptor y un código para el mensaje transmitido (p. 94). Precisado este concepto es pertinente indicar que, según la informática básica, un *software* "es el conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento de un equipo" (GCFGlobal, s.f., párr. 2).

De las anteriores definiciones se puede colegir que, en esencia, interceptar comunicaciones no es más que capturar un mensaje que se produce entre un

emisor y un receptor; esto también se puede realizar mediante un *software* o un programa malicioso, al realizar la infiltración de un equipo o un sistema informático sin consentimiento para obtener toda la información que circule por este, de ahí la importancia para las autoridades de obtener las evidencias del delito, la ubicación de procesados, o, en su defecto, anticiparse a los movimientos de organizaciones criminales.

El tema de la interceptación de comunicaciones no es nuevo y su génesis se pierde a lo largo de la historia de la humanidad; por ejemplo, en Francia Luis III y el Cardenal Richelieu crearon el *Cabinet Noi*r (cámara negra) para interceptar cartas personales consideradas sospechosas hasta 1790, cuando la Asamblea Nacional Francesa proclamó la inviolabilidad de correspondencia y dispuso abolir ese instrumento. Surgió, de esta manera, el reconocimiento al secreto de la correspondencia que luego se extendió a toda forma de comunicación (Casablanca, 2015).

Así mismo, dos grandes sucesos en los que se resaltó la importancia de la interceptación de las comunicaciones fueron: el primero, como producto de la invención del teléfono en 1876 y la disputa en torno a quién fue su inventor, entre Elisa Gray, Alexander Graham Bell y el italiano Antonio Meucci, que terminó de resolverse en junio de 2002 cuando la Cámara de Representantes de los Estados Unidos reconoció que fue Meucci el inventor del mismo (Salazar, 2014, p. 89).

El segundo, se presenta con el advenimiento de las dos grandes guerras mundiales, en las que se hacía necesario capturar los mensajes del oponente. Para 1918, las tropas alemanas habían logrado interceptar las comunicaciones del ejército de los Estados Unidos, descifrar sus códigos y tomar decisiones rápidas, esta situación fue solucionada por el ejército americano mediante el establecimiento de interlocuciones entre dos soldados de la tribú *Choctaw* que hablaban su lengua nativa (Winterman, 2014). A su vez, durante la Segunda Guerra Mundial, el ejército británico conformó un "grupo conocido como los 'interceptores voluntarios', unos 1500 aficionados a la radio, reclutados

para monitorear las comunicaciones de los nazis y sus aliados antes de que llegaran a su destino" (Moskvitch, 2013, párr 3).

Posterior a ello, con el inicio de la Guerra Fría después de 1945, se celebró un pacto para intercambio de información entre el Reino Unido y los Estados Unidos conocido como UKUSA, al que después se adhirieron otros países. A partir de los años 70, se transmitieron hacia la tierra señales de radio y teléfono captadas por los satélites de escucha y observación que, posterior a eso, terminarían conformando la red de espionaje y análisis para el monitoreo de comunicaciones más grande del mundo, al que se le dio el nombre de ECHELON (Proyecto PV, s.f.).

Con el uso de las nuevas tecnologías, el tema de la interceptación de las comunicaciones sigue en auge, por lo que al día de hoy se pueden encontrar compañías dedicadas al desarrollo y la comercialización de *software*; por citar algunos, la gigante italiana *Hacking Team* que desarrolló tecnología de punta para interceptar todo tipo de comunicaciones; *Kaymera* y el sistema *Verint* 12*,* estos, debido a su especialización en la creación de *software* y al pensar en su crecimiento en Latinoamérica, situaron sus ojos en Colombia como sede local para su oficina (Chaves, 2014). También, el *software Spyera* es utilizado para la interceptación de teléfonos móviles, tabletas y computadoras; sobre su funcionamiento y legalidad se habla en el segundo capítulo.

La interceptación de comunicaciones en nuestro país.

En este contexto, Colombia posee dos sistemas alternos en esta materia: uno, conocido como ESPERANZA que hoy es denominado como la Sección de Control Telemático, operado por la Fiscalía General de la Nación; y, otro, la Plataforma Única de Monitoreo y Análisis o Sala PUMA (según sus siglas), operada por la Policía Nacional. Al respecto, conviene aclarar que la Sala PUMA opera bajo estrictas regulaciones y de forma legal; es más, las interceptaciones allí realizadas se coordinan bajo la dirección de la Fiscalía General de la Nación como lo ordena la Constitución Nacional en su artículo 250 inc. 4.º num. 2.º.

El sistema de interceptación de la Fiscalía General de la Nación (o Sección de Control Telemático) cuenta con diferentes grupos que se encuentran estructurados de la siguiente manera: Grupo de Análisis y Tratamiento de la Información; Grupo de Apoyo a la Ubicación; Salas de Recepción y Análisis de las Comunicaciones Interceptadas; Secretaría Común y, por último, el Grupo de Soporte Técnico. Dentro de dichos grupos, se destacan las Salas de Recepción y Análisis de las Comunicaciones Interceptadas, que se identifican con nombres como: GRANATE, DIAMANTE, ORO, BRONCE, MOSTAZA, JASPE y CIAN; además, también operan las salas ubicadas en las seccionales de las distintas capitales del país, a las que se les asignan las interceptaciones en los ámbitos regional o departamental (Resolución 0020 de 2016).

El objetivo de la Sección de Control Telemático se cumple con el apoyo de un proveedor de servicios de telecomunicaciones, lo cual le permite a la Fiscalía conectar los servidores de los proveedores para, de esta forma, recibir y descomponer en paquetes de llamadas las comunicaciones, con la finalidad de transmitirlas a una sala de interceptación; ello se hace por intermedio del Sistema de Interceptación de las Comunicaciones de la Fiscalía General de la Nación y el Departamento de Interceptación de las Comunicaciones (DIC), ente encargado de enrutar las líneas interceptadas a las diferentes salas de recepción de las comunicaciones (Resolución 0-1037 de 2016). Así mismo, agréguese, para llevar a cabo esas tareas la Fiscalía General de la Nación utiliza como una de sus herramientas de interceptación los denominados *software Target* 360 y *Pen-link,* este último, según se dice en su página de internet, aduce tener una experiencia de 30 años en el negocio de los sistemas de datos de comunicaciones sin aportar mayor información pública al respecto (Penlink, 2020).

En relación con el sistema de interceptación de comunicaciones operado por la Policía Nacional, la Sala PUMA, debe decirse que él monitorea a la vez la red fija, la red móvil y el ISP (*Internet Service Provider*), en el cual quedan comprendidos los servicios de correo electrónico, voz sobre IP, chats, *BBM* (*BlackBerry Messenger*), *WhatsApp* y, en general, todos los servicios de datos.

Así las cosas, a título de ejemplo, cuando se quiera monitorear un celular solo es necesario marcar el número del móvil del objetivo y el sistema captura en tiempo real el tráfico de voz, datos, fotos, chats en diferentes plataformas como "*Skype*, *Line*, *Facebook* y *Google*, entre otros" (Adalid, 2016, párr. 1).

Desde luego, la Sala PUMA está dotada de un sistema mucho más avanzado que la Sección de Control Telemático de la Fiscalía; sin embargo, es operado solo por personal perteneciente a la Policía Nacional (Privacity International, 2015). Este sistema data del año 2013, pero se habla de él desde el 2010 de acuerdo con el proceso de selección abreviada PN DIRAF SA 013 de ese año, llevado a cabo con el objeto de realizar actualización y mantenimiento a la plataforma (DIRAF, 2010).

Según uno de los mayores expertos en tecnología del país y presidente ejecutivo de Adalid Corp., Andrés Guzmán Caballero, el *software* utilizado por el sistema PUMA monitorea "casi en tiempo real, todas las comunicaciones, es decir, llamadas entrantes y salientes, mensajes de *WhatsApp*, *Snapchat*, *Facebook*, *Skype*, correos electrónicos, en una palabra, todo" (Orozco, 2015, párr. 3). Así las cosas, no cabe duda de que la plataforma PUMA tendría una mayor capacidad para interceptar comunicaciones que la Sección de Control Telemático de la Fiscalía, antes llamada Sala Esperanza, según se dijo en precedencia.

Ahora bien, respecto a la interceptación telefónica, el país ha sido presa de varios escándalos, entre los cuales cabe recordar estos: las llamadas "chuzadas" del DAS en las que se hablaba, por ejemplo, de una carpeta denominada control de escuchas, que contenía prueba de correos electrónicos interceptados de manera ilegal (Sent. Radicado 2010-000020, Juzgado 3.º Penal del Circuito Especializado de Descongestión de Bogotá), para lo cual el *software* existente podría realizar tareas como esa pero de manera legal. También, la batahola del jáquer Andrés Sepúlveda, o las realizadas con concurso de los militares a través de su sala Andrómeda; y, en fin, la compra y utilización de los servicios de la empresa *italiana Hacking Team* por parte de la Policía Nacional y su sala PUMA. Por ello, si hoy se pusieran como patrón los precitados casos

con la finalidad de hacer un debate público encaminado a introducir como mecanismo de interceptación de comunicaciones un *software* con mucha más capacidad, este proyecto no tendría muchos adeptos.

No obstante, un *software* como herramienta de interceptación telefónica podría ser de gran ayuda en investigaciones criminales de gran calado para las cuales los medios tradicionales no son suficientes en la búsqueda de la evidencia, puesto que la indagación se debe realizar no solo en los medios físicos sino en el mundo digital, debido a que la forma de comunicarse cambia en la misma medida en que avanza la tecnología. Según la Corte Constitucional, el derecho es una ciencia en constante cambio y evolución de acuerdo a cómo se desarrolla la sociedad; esos cambios se observan en varios aspectos, entre los cuales deben mencionarse el cultural, el tecnológico, el económico y, en razón a esto, pueden ser apreciados como algo que es capaz de cambiar, transformar o adaptarse (Sent. T-043 de 2020, CConst.).

Por ello, se debe estar abierto a los nuevos cambios y paradigmas dado que la tecnología evoluciona a una velocidad gigantesca en comparación con la velocidad con la cual avanza la ley. Así las cosas, ello se debe hacer sin dejar de lado la finalidad de protección a los bienes jurídicos propia del Derecho Penal que, como bien lo indica Velásquez (2021), son bienes o valores que por su importancia el legislador ha erigido en intereses merecedores de especial protección (p. 65). Desde luego, si bien es cierto que hay cambios a menudo en la legislación y en la jurisprudencia, muchas de esas variaciones son paquidérmicas y vetustas; la ley sigue viviendo en el pasado, en contraste con los nuevos avances tecnológicos que quedan sin regular. Al respecto, es menester citar como ejemplo el proyecto de ley confeccionado y presentado al Congreso de los Estados Unidos, luego del ataque del 11 de septiembre, y que –posteriormente– se convirtió en la legislación conocida como *Patriot Act* o Ley Patriota promulgada por el presidente George W. Bush, mediante la cual se le otorgó una mayor capacidad a las autoridades y servicios de seguridad para realizar operaciones de vigilancia e intervenir las comunicaciones (Lobe, 2001, p. 59).

Desde luego, este estudio no busca hacer críticas al sistema existente sino sembrar la inquietud en la comunidad académica en torno a la necesidad de apoyarse en la tecnología para combatir las diversas formas de criminalidad puesto que, con el tiempo, ellas se hacen cada vez más especializadas en su forma de delinquir a cuyo efecto se valen de grandes recursos económicos y tecnológicos.

El *software* como herramienta de interceptación

Funcionamiento del *software* de interceptación y nivel de acceso a las comunicaciones

Aquí debe hacerse hincapié en algunos tipos de *software* máxime si se tiene en cuenta que el mercado forense digital se ha segmentado sobre componentes de *hardware* y *software* (Markets Insider, 2018). Entre estos el "RCS", desarrollado por la empresa italiana *Hacking Team* y creado por la compañía *Spyera* como *software* de monitoreo de comunicaciones. A tal efecto, se debe iniciar con una breve explicación sobre la forma como funcionan ambos sistemas, el nivel de acceso a las comunicaciones y las diferencias entre estos, para ejemplarizar.

Acerca del funcionamiento del *Remote Control System* (RCS o Sistema de Control Remoto), desarrollado por *Hacking Team*, Pérez (2016) resaltó que también se le conoce con los nombres de Galileo y DaVinci, fue creado con el objetivo legal de combatir el crimen, al distinguir al RCS de su competencia por su acceso a todo tipo de comunicaciones y archivos en celulares y computadoras. Este tipo de *software* puede acceder a contraseñas, mensajes, correos, contactos, cámara, micrófono, ubicación geográfica y distintas aplicaciones, esto es prácticamente a todo lo que transcurre en el equipo inoculado (Pérez, 2016).

Respecto al funcionamiento del *software Spyera*, en su página oficial de internet se indica lo siguiente:

> *Spyera* es un software de monitoreo de teléfono celular indetectable que se instala en el dispositivo de destino. Después de la instalación *Spyera* empieza a capturar registros y cargarlos en una cuenta web segura. Puede iniciar sesión en la cuenta *web* segura por cualquier navegador *web* (Spyera, 2019, párr. 26).

De igual manera, allí se explica que el mismo está en la capacidad de supervisar llamadas, abrir la cámara de forma remota, entrar al GPS (*Global Positioning System*), espiar fotos, videos, correos y mensajes, y acceder a toda la información de un teléfono celular, tableta o computadora. Desde luego, la gran diferencia entre el *software* RCS, desarrollado por *Hacking Team,* y el *software* creado por *Spyera* radica que en este último no es posible la instalación remota, mientras que el RCS sí lo consiente. Además, *Hacking Team* aduce tener como política empresarial, vender su *software* solo a organizaciones gubernamentales; *Spyera*, por el contrario, es accesible al público en general.

En este punto, es menester recordar el alto nivel de acceso a las comunicaciones por parte del *software,* por lo cual no se debe olvidar que la doctrina alemana diferenció desde hace tiempo las prohibiciones de producción de pruebas entre absolutas y relativas: "[…] la producción de prueba absoluta no permite bajo ninguna consideración la práctica probatoria como, por ejemplo, la interceptación de las comunicaciones entre el defensor y el imputado" (Guerrero, 2009, p. 156); por esta razón, deberá tenerse en cuenta el profundo nivel de acceso a las comunicaciones por parte de los *software* analizados (Hacking Team y Spyera), a fin de no afectar el precitado derecho constitucional entre defensores y procesados; ese es uno de los principales retos a resolver cuando se trata del uso y empleo de estos *software*.

Además, cabe destacar que por el nivel de acceso a las comunicaciones del *software* se podrá dar solución, entre otros aspectos, al del conocido lenguaje cifrado o aparente, que, como lo resaltó la Corte Constitucional, no es más que la utilización de un lenguaje común en clave o disfrazar la realidad (Sent. C-586 de 1995, CConst.), máxime si sobre ello siempre habrá una gran controversia en el tema probatorio. También, es importante resaltar que a diario se documentan las vidas y lo que cada persona hace en los teléfonos y

portátiles (Cope *et al*., 2017), independiente del lenguaje utilizado, cuando se emplean ciertos términos en el argot criminal para ordenar o realizar determinadas tareas, de las cuales siempre queda trazabilidad al respecto. Sin embargo, en este punto es indiscutible la función del *software* para solucionar la anterior objeción sumada a la posibilidad de identificación del usuario del equipo utilizado.

La legalidad de la interceptación mediante *software*.

Al respecto, debe recordarse que según *Wainwright* (2016) debe crearse una matriz o un documento en el cual se enuncie "[…] si hay leyes aprobadas para permitir la extradición y la escucha telefónica y qué tan estrictas son las reglas […]" (p. 143); ello posibilita inferir que el autor equipara el funcionamiento de las organizaciones criminales con el ejercicio de una empresa que tiene desarrollo económico legal. Además, da por sentada la necesidad de disponer de herramientas adecuadas para contrarrestar el accionar criminal de aquellas, razón por la que el *software*, como instrumento de interceptación de comunicaciones, podría ayudar al desmantelamiento de estas redes criminales lo que sería poco eficaz a través de otros medios pero sin dejar de lado su estricta regulación legal.

Por supuesto, no son pocas las voces en contra de la utilización del *software* para interceptar, como lo manifiesta Pérez (2016), al mencionar que "programas de espionaje tan invasivos como el de *Hacking Team* se prestan a abusos y violaciones de derechos humanos" (p. 71). En este sentido, la Fundación Karisma (2015) critica la contratación del Estado colombiano con la empresa italiana y la rechaza, a cuyo efecto se escuda en la filtración de la que fue objeto *Hacking Team*. A su vez, el Centro de Estudios Jurídicos y Sociales DeJusticia (2015), dedicado al fortalecimiento de los derechos humanos, también se pronuncia al respecto: "*Hacking Team* es una cuestionada compañía italiana que comercializa herramientas tecnológicas de espionaje y de invasión a la intimidad" (párr. 1).

Como es obvio, nuestra pretensión no es defender una u otra empresa desarrolladora de *software* sino poner de presente que se pueden interceptar llamadas y sistemas de datos por métodos distintos a la telefonía ordinaria. Desde luego, de cara al debate sobre la legalidad del *software* como instrumento de interceptación, debe decirse que en nuestra legislación no se encuentra regulado tácita ni procedimentalmente ese curso de actuación; pero, el artículo 250 de la Constitución Política en su inc. 4.º num. 2.º, ya citado, señala como función de la Fiscalía General de la Nación la de "adelantar interceptaciones de comunicaciones" (Const. Pol., 1991), con un control posterior ante el juez que ejerza la función de control de garantías.

En este sentido, el Código de Procedimiento Penal en su artículo 235 indica que el fiscal, con la finalidad de buscar elementos materiales probatorios y ubicar procesados, podrá ordenar que se intercepten comunicaciones mediante "grabación magnetofónica o similares las comunicaciones" (Ley 906, 2004) que se cursen por cualquier red de comunicaciones por el término de seis meses y solo deberá someterse al control previo de legalidad por parte del juez de control de garantías. El anterior procedimiento está sometido a un control posterior como lo dispuso el artículo 237 de la ley adjetiva.

Además, el artículo 301 de la Ley 600 de 2000, Código de Procedimiento Penal que coexiste junto a la Ley 906 de 2004 para rituar las actuaciones con ocasión de las conductas anteriores al primero de enero de 2005 y las realizadas, en cualquier tiempo, por los aforados constitucionales, señala el procedimiento de interceptación de comunicaciones en el estatuto procesal. Al respecto, es de anotar que tanto el artículo 235 de la Ley 906/2004 como el artículo 301 de la Ley 600/2000, muy de espaldas a la realidad, hicieron referencia a la interceptación de comunicaciones mediante grabación magnetofónica, como si no fuera evidente que el magnetófono es un aparato condenado al ostracismo dado que su función es análoga en su totalidad; ello contrasta con un mundo en el que todo es digital y que aún espera nuevas tecnologías. No obstante, el artículo 235 de L. 906/2004 sí dejó de lado la comunicación radiotelefónica que aún se conserva de manera literal en la L. 600/2000.

De igual forma, la técnica de investigación por la cual aboga el artículo 235 de la Ley 906/2004 supone que la interceptación de comunicaciones constituye un acto de investigación diferente al del artículo 236 de la misma normativa, esto es, la recuperación de información producto de la transmisión de datos a través de las redes de comunicaciones. Ello, porque en esta última se hace necesario aprehender el equipo terminal, el dispositivo o el servidor, con la finalidad de que un perito o experto en informática forense recuperen la información y, posteriormente, devuelvan el equipo incautado. Mientras que la interceptación propuesta en la presente investigación, mediante *software*, busca que se intercepten las comunicaciones en tiempo real, sin necesidad de tener acceso al equipo físico, obteniendo la información de interés que curse por la red de comunicaciones; además de que esa actividad puede efectuarla el investigador o el analista de comunicaciones sin la calificación de perito.

Ahora bien, con respecto a la necesidad de la autorización por parte del juez de control de garantías en defensa de los derechos de los ciudadanos, la Corte Constitucional ha dicho que el órgano persecutor puede interceptar comunicaciones con el respectivo control posterior ante el juez de garantías, con lo cual dejó zanjado el asunto de la autorización previa para el tema (Sent. C-336 de 2007, CConst.). No obstante, como se ha dicho antes en el texto sí se hace necesaria la autorización previa y el control posterior por parte del juez de control de garantías, en aras de blindar a los ciudadanos, garantizar la protección de sus derechos y no dejar al arbitrio de una de las partes en litigio esta prerrogativa. Máxime si se tiene en cuenta el uso de una herramienta tan invasiva a la intimidad como lo puede ser el *software* de interceptación.

Ahora bien, la cuestión a responder es lo siguiente: ¿qué se puede exponer sobre la interceptación de comunicaciones por medio de *software*? Nada dicen al respecto la carta política y la ley procesal, y ello es entendible porque en ese momento no existía en el país el *software* para interceptar comunicaciones o solo se encontraba en manos de potencias mundiales y, bien se sabe, los avances jurídicos referentes a medios tecnológicos llegan a una velocidad muy pausada.

Por lo anterior, la Corte Constitucional ha empezado a referirse a ciertos temas tecnológicos como el de los pantallazos de *WhatsApp* (Sent. T-043 de 2020, CConst.); sin embargo, la respuesta al interrogante anterior se podría hallar en otra parte. En efecto, la Constitución Política en su artículo 250 inc. 4.º num. 2.º, varias veces citado, autoriza a la Fiscalía para adelantar interceptaciones de comunicaciones y ello, como se dijo previamente, no es más que capturar un mensaje entre personas. Este artículo, recuérdese, fue desarrollado en la Ley 906 de 2004 en su artículo 235, según el cual el fiscal con la finalidad de buscar evidencia y ubicar procesados podrá ordenar que se intercepten, mediante grabación magnetofónica o similares, las conversaciones que se cursen por cualquier red de comunicaciones; así las cosas, estaría indicando la ley que ello no solo se puede hacer mediante grabación magnetofónica sino también por medios de similares (Ley 906 de 2004).

Al respecto, téngase en cuenta que según la gramática española el valor semántico de la conjunción "y" es combinatorio: ejemplo "¿quiere café y leche?"; mientras que la conjunción "o" es disyuntiva, ejemplo: "¿quiere café o leche?" (Castelli, 2012); por ello, tal construcción abre el espectro para que la interceptación se pueda hacer por la mejor forma que ofrezca la tecnología, siempre y cuando se realice de manera lícita, legal y procedimental. Así las cosas, al día de hoy se puede interceptar de forma legal en investigaciones penales: llamadas de voz, mensajes de texto, comunicaciones *BlackBerry Messenger* (BBM), archivos como fotos, videos y notas de voz, ubicación de personas mediante celdas, entre otros; esto lo permiten la ley y la tecnología vigente en cualquiera de las salas de la Sección de Control Telemático, sin estudiar de fondo el potencial de la Sala PUMA de la Policía Nacional.

En auxilio a lo expresado, la Ley 1908 de 2018 introdujo en su artículo 28 el desarrollo de un protocolo entre gobierno, Fiscalía y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), para hacer frente al crimen organizado, apoyándose en la tecnología lo que incluye, de manera categórica, el *software* y se abre un espectro para interceptar comunicaciones con tecnología de punta, en el que se indica que, en

coordinación con los anteriores entes, se capacitará y adquirirá tecnología que "permitan combatir de manera eficaz y oportuna a los Grupos Delictivos Organizados (GDO), Grupos Armados Organizados (GAO)" (Ley 1908, 2018, art. 28).

De igual forma, es loable destacar la regla de exclusión proveniente de la justicia americana, desde el caso *Weeks* vs. Estados Unidos, en el que fue revocada la condena de una persona, dado que la prueba se soportaba en evidencia recolectada en su vivienda sin previa orden de registro (Weeks vs. Estados Unidos, 232 US 383 1914). En esa ocasión se vulneró la IV Enmienda de la Constitución de los Estados Unidos (Legal Information Institute, s/f). Esta regla de exclusión a registros, que luego fue acogida para el contenido de las interceptaciones telefónicas desde los casos *Olmstead* vs. Estados Unidos de América en 1928 (Olmstead vs. Estados Unidos, 277 US 438 1928) y posterior a estos, el caso de *Katz* vs. Estados Unidos de América en 1967, cuando la corte extendió no solo a espacios físicos la protección de la IV Enmienda sino a la privacidad de las personas y sus comunicaciones telefónicas (Katz vs. Estados Unidos, 389 US 347 1967).

En ese orden de ideas, la utilización de *software* como herramienta de interceptación de comunicaciones y similares sería legal e innovadora al tener en cuenta que el objeto material de las interceptaciones son las comunicaciones de otras personas sin interesar el medio tecnológico utilizado para su transmisión (Casanova, 2014). Por ello, debido a que el tema es poco explorado en el país además de la eficiencia que presentaría el *software* en la lucha contra la delincuencia, aunque la Ley 1908 de 2018 versó sobre el crimen organizado, se debería dar importancia al estudio de este en la comunidad académica.

Ahora bien, cabe preguntar: ¿Qué tipo de evidencia se puede obtener con el *software* de interceptación de comunicaciones? y ¿cómo se ingresa a un proceso penal la información obtenida mediante el *software* de interceptación? Respecto a la interceptación de comunicaciones telefónicas, Cruz (2019) señala que "los resultados que arroja esta actividad probatoria constituyen lo

que conceptualmente se conoce como evidencia digital y, más exactamente, como 'mensaje de datos" (p. 283). Por eso, debido a lo invasivo que resulta para la intimidad personal, el secreto de las comunicaciones y el derecho de la no autoincriminación amparados por la Constitución, para implementar el *software* de interceptación de comunicaciones es necesario hacer un análisis minucioso del tipo de prueba que podría llegar a ser (Asamblea Nacional Constituyente).

Al respecto, recuérdese que la Ley 527 de 1999 recoge una modalidad traída de la Ley Modelo UNCITRAL (*United Nations Commission for the Unification of International Trade Law*), mediante la cual las Naciones Unidas señaló las bases en materia de comercio electrónico (Agencia Nacional de Defensa Jurídica del Estado, 2017); en esa normativa se definió y reglamentó el acceso y el uso de los mensajes de datos en su artículo 2.º: "Mensaje de datos: la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax".

¿Por qué se manifiesta la interceptación de comunicaciones mediante *software* como mensaje de datos? Para responder a la anterior cuestión, se observó que la información se genera por medios electrónicos, intercambio de datos por internet, correo electrónico y demás, en los que se podrían ubicar las cientos de aplicaciones (*app*) que se utilizan en la actualidad para comunicarse mediante mensajería, audio y video, como *WhatsApp* que utiliza un cifrado de extremo a extremo, lo cual hace que haya una trazabilidad del recado y se sepa si el mensaje es nuevo o fue reenviado (Rodríguez & Schoen, 2020), *Telegram*, *Instagram*, entre otras. A ellas el *software* las lograría captar a diferencia de la interceptación tradicional actual en la que estas comunicaciones se perderían del radar de las autoridades.

Aunado a lo anterior, dispositivos como celulares, tabletas y computadoras portátiles se utilizan hoy en día para muchas otras actividades en la vida cotidiana, por ejemplo, revisar correos electrónicos, tomar fotografías,

navegar en internet, realizar transacciones comerciales, datos de ubicación, entre otros (Ali *et al*, 2017), por todo esto la efectividad de un *software* para obtener medios de prueba sería indiscutible.

Respecto a la regulación legal ella encuentra su sustento en las siguientes disposiciones: Ley de Comercio Electrónico (Ley 527 de 1999), el Código General del Proceso (CGP) o la Ley 1564 de 2012; artículos 243 al 274 de la Ley 1564 de 2012; y, para el ámbito penal, el Código de Procedimiento Penal, Ley 906 de 2004, artículos 275 literal G, referente a que los mensajes de datos son elementos materiales probatorios. El artículo 382, que versa sobre los medios de conocimiento, indica que la prueba documental, los elementos materiales probatorios, la evidencia física y cualquier medio técnico, son medio de conocimiento. Además, en el artículo 424 num. 2.º, aparecen las grabaciones magnetofónicas y en el num. 7.º los mensajes de datos, con lo cual se aduce que, para efectos de la ley adjetiva, las grabaciones y los mensajes de datos son prueba documental (Ley 906 de 2004).

Continuando con el análisis, se debe dejar en claro que el artículo 243 del CGP enunció las distintas clases de documentos; entre ellos se tienen como documentos los mensajes de datos, al igual que lo citó la Ley 527 de 1999 en su artículo 2.º, situación que quedó resuelta mediante un pronunciamiento de constitucionalidad (Sent. C-604 de 2016, CConst.). De acuerdo con el artículo 245 del CGP los documentos se deben aportar en original o en copia y cuando se provea una copia se tiene que manifestar dónde se encuentra el original, en caso de tener este conocimiento (Ley 1564 de 2012). Al observar los principios de neutralidad tecnológica y equivalencia funcional, se entiende que los mensajes de datos son algo inmaterial y deben ser llevados en algo material para su presentación.

Para el caso penal, el Código de Procedimiento Penal en su artículo 275 literal G, señala que los mensajes de datos son documentos. Por su parte, el artículo 382 indica que la prueba documental es un medio de conocimiento; a su turno, el artículo 424 expresa que se entiende por prueba documental las grabaciones magnetofónicas y los mensajes de datos, incluso se enuncia que,

para este Código, las grabaciones y los mensajes de datos son documentos. Para finalizar, el artículo 431 alude al empleo de los documentos en el juicio, en el que deben ser proyectados o exhibidos por cualquier medio para que puedan llevar al conocimiento claro del hecho, referido en el artículo 432.2.

Con respecto a la aportación de la prueba electrónica en el procedimiento penal Sánchez (2016) afirma que la aportación de imágenes o sonidos que lleve a demostrar una actividad ilícita, debe entregarse mediante grabación en un disco compacto (*CD*), disco versátil digital (*DVD*) o en el bus universal en serie, más conocido por su sigla (*USB*), acompañada de una trascripción escrita. En ese orden de ideas los mensajes de datos obtenidos mediante un *software* deben seguir el procedimiento establecido para la interceptación de comunicación telefónica, a fin de ser incorporados como prueba documental en un proceso penal. Por esta razón, no existiría una mayor diferencia coyuntural con lo existente al día de hoy. Que, si se debe distinguir o no con la evidencia electrónica o digital, ya será motivo de estudio de otros trabajos más amplios sobre la materia.

Ventajas del *software* frente al actual sistema de interceptación de comunicaciones.

Autores como Gómez (2017) afirman que "este acto de investigación tiene una efectividad tremenda en la lucha contra los grandes crímenes (los cometidos por la criminalidad organizada, los de narcotráfico, terrorismo, corrupción, etc.)" (p. 180). Así, hace alusión al crimen organizado en sus diferentes modalidades que afectan, de manera circunstancial, bienes jurídicos colectivos e individuales y toma una postura sobre la efectividad de las interceptaciones. Por ende, si hoy en día esas comunicaciones mutan al plano tecnológico, lo más coherente para que esta efectividad se mantenga es que las autoridades muten a este campo, con la finalidad de hallar la evidencia en la que se encuentra y de no buscarla donde poco queda.

En artefactos como los celulares, las computadoras o las tabletas, en los que la interceptación tradicional no llegaría en búsqueda de evidencia,

el *software* conseguiría tener acceso a correos electrónicos, cámaras de los dispositivos e incluso micrófonos de estos; esta herramienta permitiría identificar a cualquier persona; con ello, zanja la eterna dicotomía entre ente acusador y defensa en torno a si la persona que habla en la interceptación es o no quien la Fiscalía identifica. Además, previene errores judiciales en ese ámbito y llega al accionar delictivo en cualquier lugar en el que la persona se encuentre.

Respecto al tema costo-beneficio de un *software*: al realizar los actos de investigación y vigilancia las 24 horas del día, mediante el mismo, sería significativo el aporte a la interceptación de comunicaciones, en comparación con el sistema tradicional, por ejemplo, si el Estado decidiera permear las redes delincuenciales por medio de la figura de un agente encubierto, el *software* lo reemplazaría las 24 horas del día. Así mismo, el *software* de interceptación proporcionaría la ubicación exacta de la persona interceptada, dato clave en las investigaciones; es más, esa información de geolocalización puede suministrar pruebas muy sólidas si se trata de manera adecuada (Casey, 2018).

No se puede obviar que toda medida de vigilancia se debe asentar sobre una ley que sea específicamente precisa, en especial por el riesgo que se corre de abusar de un sistema de vigilancia secreta y el continuo avance de la tecnología para realizar estas labores (Rivera & Rodríguez, 2015). Respecto a esa necesidad de delimitación de las herramientas, las autoridades pueden tener instrumentos legales de interceptación, sujetos a restricciones como las que se encuentran en la protección de datos (Centro de Estudios en Libertad de Expresión y Acceso a la Información, s.f.). El Estado es el que debe implementar medidas cuando se interfieran derechos a la privacidad y más si hay ausencia de una ley regulatoria (Fundación Karisma, 2013).

Una observación más debe hacerse: las palabras *interceptación* y *monitoreo*, que han sido empleadas aquí, se distinguen conceptualmente en la Ley de Inteligencia y Contrainteligencia (Ley 1621 de 2013), en cuyo artículo 17 se indica que las actividades de inteligencia y contrainteligencia comprenden las de monitoreo del espectro electromagnético, mientras que la interceptación

de comunicaciones es propia de procedimientos judiciales de indagaciones o investigaciones adelantados usualmente por la Fiscalía General de la Nación.

Una mirada al derecho comparado sobre la interceptación de mensaje de datos

Ahora bien, de cara a tener una visión más omnicomprensiva de la materia que nos ocupa, es importante hacer una comparación con tres legislaciones prototípicas como se muestra a continuación de cara a evidenciar la viabilidad en el régimen legal colombiano en materia del uso de software como herramienta de monitoreo de sistemas de datos.

España.

Con la modificación a la Ley de Enjuiciamiento Criminal mediante la Ley Orgánica 13/2015 del 5 de octubre, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (L.O. 13/2015), se amplió la obligación de colaborar por parte de todos los prestadores de servicio con los jueces y la policía judicial para permitir el registro remoto de equipos informáticos de uso y almacenamiento (Lecuit, 2018). Ello, sin duda, denotó un mayor compromiso y apoyo a los nuevos sistemas de monitoreo remoto. A su turno, la Ley de Enjuiciamiento Criminal en su artículo 588 ter b., expresa que los datos electrónicos son todos los que se generan a través de comunicaciones electrónicas; así mismo, en su artículo 588 *septies* a., hace referencia a la utilización de software en la investigación e indica que se debe obtener autorización judicial previa para su utilización y que el lapso es solo por el término de tres meses. Además, la instalación del *software* debe estar precedida por la autorización de un juez y el mismo debe permitir acceder de forma remota al contenido de ordenadores o dispositivos electrónicos, sin el consentimiento de su titular o quien lo use, siempre y cuando sea uno de los delitos de los enlistados por el legislador.

Así las cosas, no cabe duda de que en esta legislación se hace uso del *software* de monitoreo de comunicaciones bajo ciertas prerrogativas como lo son la autorización judicial, un término de tres meses y la existencia de una lista de delitos para su utilización.

México.

Por otro lado, los Estados Unidos Mexicanos en su Código Nacional de Procedimientos Penales de 5 de marzo de 2014, trae el capítulo dedicado a los actos de investigación, desarrollados desde el artículo 291 al 303. Este código, en su artículo 252, enuncia los actos de investigación que requieren autorización previa del juez de control, e indica: la exhumación de cadáveres; las órdenes de cateo; la toma de muestras de fluido corporal, vello o cabello; extracciones de sangre u otros análogos; y la intervención de comunicaciones privadas y correspondencia (Congreso General de los Estados Unidos Mexicanos, 2014).

Posterior a esto, en su artículo 291 indica que la intervención de comunicaciones privadas arropa todo tipo de comunicaciones, incluso las provenientes de los nuevos avances tecnológicos, cuando se realice intercambio de archivos electrónicos como audios y vistos, así se den en tiempo real o con posterioridad. A partir de ello, se puede observar el desarrollo de programas fruto de la evolución tecnológica como puede ser el software de monitoreo dado que se pueden intercambiar datos, audio, videos, mensajes y archivos electrónicos.

En fin, parece también claro que en la legislación procesal mexicana se hace uso del *software* de interceptación de comunicaciones bajo las premisas de la legislación española, con la autorización judicial previa, pero con una variación en cuanto al término puesto que ya no es de tres meses sino de seis.

Reino Unido.

En el año 2000 se aprobó la *Regulation of Investigatory Powers 2000* (RIPA) o Ley de Regulación de los Poderes de Investigación que introdujo regulaciones a las órdenes de interceptación, entre estas, lo relativo a su contenido, a su duración y sus efectos; su vigencia comenzó el 2 de octubre de 2000. La RIPA prevé la adopción de códigos de práctica para interceptar comunicaciones por medio del secretario de Estado; en su artículo 71 num. 1.º indica el sometimiento o acatamiento de los códigos para poder llevar a cabo las interceptaciones de comunicaciones (Casanova, 2012).

Estas intervenciones son autorizadas de manera judicial (Sección 5 RIPA) y deben ser necesarias y proporcionales a lo que se quiere lograr; además, debe seguir los lineamientos del artículo 8.º de la Convención Europea de Derechos Humanos (CEDH), lo cual significa que la intervención debe ser por un periodo de tres meses y se debe manifestar el tipo de comunicaciones que se pretende monitorear. En el tipo de comunicaciones tienen cabida la interceptación por medio de *software* con las formalidades antes requeridas.

Así mismo, se debe precisar que las interceptaciones en la legislación británica son una excepción en el proceso penal y solo pueden ser llevadas a juicio por el fiscal o, excepcionalmente, por el juez de cara a su obligación de hacer justicia. Por lo tanto, aunque es amplio y regulado el margen de la técnica investigativa, su uso en el proceso penal no es tan común (Casanova, 2012) como en la legislación colombiana.

Con posterioridad, se aprobó la *Investigatory Powers Act* (United Kingdom, 2016) que obliga a los a proveedores de comunicaciones a mantener los registros de conexión a Internet de los usuarios (metadatos) durante un año, permitiendo el acceso remoto a ordenadores y teléfonos inteligentes para la implantación de programas de vigilancia o la descarga de información; se le conoce como la Ley de los Fisgones y entró a regir, por partes, a partir del 30 de diciembre de 2016. Esta Ley otorga poderes a las fuerzas de seguridad para solicitar la colaboración a los proveedores de comunicaciones para descifrar

cualquier comunicación de los usuarios y consolida la interceptación masiva de comunicaciones (metadatos) (Lecuit, 2018).

Conclusiones

Como resultado de lo dicho en precedencia, se puede concluir que la interceptación de comunicaciones por un método distinto a la telefonía ordinaria es viable en su totalidad, porque es legal y está permitida en la legislación vigente. Como se logró evidenciar, el *software* de interceptación es una herramienta útil para lograr el fin de una investigación, como lo es obtener evidencia para el esclarecimiento de los hechos y/o ubicar procesados, pero el uso de esta herramienta debe ser delimitado por el legislador.

En este orden de ideas, se logró establecer la necesidad de que se expida en el ordenamiento nacional una ley de interceptación de comunicaciones que abarque todas estas aristas; desde la interceptación como se conoce hoy en día, los nuevos avances tecnológicos en la materia y, por supuesto, el uso del *software* de interceptación, dado que es el fundamento del presente trabajo. Esta ley debe tomar como ejemplo práctico la Ley Orgánica 13 de 2015 de la legislación española, que es reciente e innova en la materia, además se encarga de darle un tratamiento objetivo al tema de las interceptaciones y de los nuevos avances tecnológicos, como se logró evidenciar.

También, la falta de esa normatividad se pone en evidencia máxime si se tiene en cuenta que las intervenciones a las comunicaciones son usadas con mayor frecuencia en el proceso penal y esto genera que sea necesaria la expedición de una normativa clara y precisa sobre la materia como la que se demanda, máxime si se manifiestan nuevas formas de interceptar comunicaciones como la del *software*, que –sin ese apoyo legal– quedaría en un limbo jurídico y ello se prestaría a todo tipo de interpretaciones.

Para el caso europeo, el término de tres meses es más que suficiente para interceptar una comunicación, en el derecho nacional seis meses prorrogables

es un lapso demasiado prolongado en el tiempo porque afecta todo tipo de derechos; por este motivo, se debería establecer un menor tiempo de interceptación de las comunicaciones más aún en el uso del *software,* al ser una herramienta mucho más potente y con menos limitaciones técnicas que los actuales sistemas.

De igual forma, la necesidad de un control previo y posterior para interceptación con *software* se hace no solo evidente sino indispensable, con la finalidad de no vulnerar derechos fundamentes y, al tener en cuenta el alto nivel de acceso a las comunicaciones, aplicaciones, cámaras y la ubicación de la persona interceptada. Aunado a lo anterior, en el país existe la figura del juez de control de garantías y el uso de todo tipo de interceptaciones debería estar supeditado a su respectiva autorización previa y control posterior.

En armonía con lo anterior, se debería crear una policía judicial tecnológica o policía judicial informática, que esté a la vanguardia de cualquier tipo de modalidad o *modus operandi* empleado por la criminalidad para comunicar sus actos delictivos, sobre todo si se tiene en cuenta que, con el avance de la tecnología, a futuro la mayor cantidad de evidencia a recaudar en los procesos será de carácter digital o tecnológica. Además, la policía judicial deberá ser experta en presentar esa evidencia en juicios de forma técnica, ordenada y legal.

En fin, parece claro que –acorde con la pregunta que trasunta el problema de investigación formulada al principio de este texto– sí es necesario el empleo de nuevas herramientas de interceptación para sistemas de datos, cuando se piensa en combatir la criminalidad en especial la organizada.

Referencias

Adalid (2016). *Consultorio: ¿Cómo funciona la Plataforma Única de Monitoreo (PUMA)?* https://www.adalid.com/como-funciona-la-plataforma-unica-de-monitoreo-puma/

Agencia Nacional de Defensa Jurídica del Estado (2017). *La prueba electrónica. Entrevista al experto Andrés Guzmán Caballero.* https://www.youtube.com/watch?v=8IebLRPkCU4

Ali, A., Razak, S., Hajar, S., Mohammed, A., & Saeed, F. (2017, abril 26). A metamodel for mobile forensics investigation domain. *PloS One 12* (4). https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0176223doi:10.1371/journal.pone.0176223

Alto Comisionado de las Naciones Unidas para los Refugiados [Acnur]. (1998). *Convención Europea de Derechos Humanos.* https://www.acnur.org/fileadmin/Documentos/BDL/2002/1249.pdf

Beling, E., Ambos, K., & Guerrero, Ó. J. (2009). *Las prohibiciones probatorias.* Temis.

Casablanca, P. (2015). *Las intervenciones telefónicas en el sistema penal.* Universidad de Salamanca.

Casanova, R. (2012). Las intervenciones telefónicas en Reino Unido: ¿Un modelo a seguir? *Justicia. Revista de Derecho Procesal (2),* 367-408.

Casanova, R. (2014). *Las intervenciones telefónicas en el proceso penal.* Jose María Bosch Editor.

Casey, E. (2018). Clearly conveying digital forensic result. *Digital Investigation, 24.* 10.1016/j.diin.2018.03.001

Castelli, E. (2012). *Uso de y/o: ¿correcto o incorrecto?* Gramática española: http://elblogdegramatica.blogspot.com/2012/12/uso-de-yo-correcto-o-incorrecto.html

Centro de Estudios en Libertad de Expresión y Acceso a la Información. (s.f.). *Vigilancia de la red: ¿qué significa monitorear y detectar contenidos en internet?* Universidad de Palermo. https://www.palermo.edu/cele/pdf/El-deseo-de-observar-la-red.pdf

Chaves, M. (2014). *Verint Systems planea poner una oficina en Colombia.* Empresas: https://www.larepublica.co/empresas/verint-systems-planea-poner-una-oficina-en-colombia-2135276

Congreso General de los Estados Unidos Mexicanos. (2014). *Código Nacional de Procedimientos Penales.* https://www.oas.org/juridico/PDFs/mesicic5_mex_ane_15.pdf

Cope, S., Kalia, A., Schoen, S., & Schwartz, A. (2017). *Digital Privacy at the U.S. Border. Protecting the Data on your Devices and in the Cloud.* https://www.eff.org/wp/digital-privacy-us-border-2017

Constitución Política de Colombia (1991). Asamblea Nacional Constituyente. *Diario Oficial 51478 del 25 de octubre de 2020.* Imprenta Nacional. http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Cruz, Ó. A. (2019). La interceptación de comunicaciones en el sistema procesal penal: valor probatorio para la imposición de la medida de aseguramiento. *Cuadernos de Derecho Penal N.º 21*, 249-290.

Decreto 1704 (2012, agosto 15). Por medio del cual se reglamenta el artículo 52 de la Ley 1453 de 2011, se deroga el Decreto 075 de 2006 y se dictan otras disposiciones.

Presidencia de la República [Colombia]. http://www.suin-juriscol.gov.co/viewDocument.asp?id=1334621

Dejusticia. (2015, julio 30). *Policía colombiana debe aclarar su relación con "Hacking Team"*. https://www.dejusticia.org/policia-colombiana-debe-aclarar-su-relacion-con-hacking-team/

Dirección Administrativa y Financiera de la Policía Nacional [DIRAF]. (2010). *Proyecto pliego de condiciones*. Dirección Administrativa y Financiera de la Policía Nacional [DIRAF]. https://www.dropbox.com/s/ox60fsvtv2qd710/InventarioPuma.pdf?dl=0

Fundación Karisma (2015, julio 24). Sobre Hacking Team en Colombia. https://karisma.org.co/sobre-hacking-team-en-colombia/

Fundación Karisma (2013, julio 10). *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*. Fundación Karisma. https://web.karisma.org.co/wp-content/uploads/2014/03/13Principios_es.pdf

GCFGlobal. (s.f.). Informática básica. ¿Qué es hardware y software? https://edu.gcfglobal.org/es/informatica-basica/que-es-hardware-y-software/1/

Gómez, J. L. (2015). *Los fundamentos del sistema adversarial de enjuiciamiento criminal. (Fortalezas y debilidades del Proceso Penal Acusatorio con Juicio Oral y Público. Su interpretación en América Latina, con especial referencia a Colombia)*. Ediciones jurídicas Andrés Morales.

Gómez, J. L. (2017). El proceso penal español a comienzos del siglo XXI. Diagnóstico sobre sus principales problemas y propuesta de posibles soluciones, al hilo de la lucha contra la criminalidad organizada y la persecución de los delitos de corrupción. *InDret. Revista para el Análisis del Derecho, 1*, 1-59. http://repositori.uji.es/xmlui/handle/10234/167491

Guerrero, O. J. (2009). Las prohibiciones de prueba en el proceso penal colombiano. Anotaciones de derecho comparado. En E. Beling, K. Ambos & O. J. Guerrrero: *Las prohibiciones probatorias* (pp. 153-213). Editorial Temis.

Leal, H. (2011). *Diccionario Jurídico*. Edileyer.

Lecuit, J. A. (2018). *Privacidad, confidencialidad e interceptación de las comunicaciones. CIBER elcano* No. 35, Real Instituto Elcano: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari92-2018-alonsolecuit-privacidad-confidencialidad-interceptacion-comunicaciones

Legal Information Institute (s.f.). *Legislación sobre pesquisas y confiscaciones cuarta enmienda*. https://www.law.cornell.edu/wex/es/legislaci%C3%B3n_sobre_pesquisas_y_confiscaciones_cuarta_enmienda

Ley 527 (1999, agosto 18). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen

las entidades de certificación y se dictan otras disposiciones. Congreso de la República [Colombia]. *Diario Oficial No. 43.673 de 21 de agosto de 1999*. Imprenta Nacional.

Ley 600 (2000, julio 24). Por la cual se expide el Código de Procedimiento Penal. Congreso de la República [Colombia]. *Diario Oficial No. 44.097 de 24 de julio de 2000*. Imprenta Nacional.

Ley 906 (2004, septiembre 1). Por la cual se expide el Código de Procedimiento Penal. Congreso de la República [Colombia]. *Diario Oficial No. 45.658 del primero de septiembre de 2004*. Imprenta Nacional.

Ley 1564 (2012, julio 12). Por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones. Congreso de la República [Colombia]. *Diario Oficial No. 48.489 de 12 de julio de 2012*. Imprenta Nacional.

Ley 1621 (2013, abril 17). 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 a cumplir con su misión constitucional y legal. Congreso de la República [Colombia]. *Diario Oficial No. 48.764 de 17 de abril de 2013*. Imprenta Nacional.

Ley 1908 (2018, julio 9). Por medio de la cual se fortalecen la investigación y judicialización de organizaciones criminales, se adoptan medidas para su sujeción a la justicia y se dictan otras disposiciones. Congreso de la República [Colombia]. *Diario Oficial No. 50.649 de 9 de julio de 2018*. Imprenta Nacional.

Ley Orgánica 13 (2015, 5 de octubre). De modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Jefatura de Estado [España]. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725

Lobe, J. Un país rigurosamente vigilado. En K. Lucas (Comp.): *Estados Unidos en guerra. Del miedo a la libertad vigilada* (pp. 59-61). Abya-Yala. https://biblio.flacsoandes.edu.ec/libros/digital/46589.pdf

Markets Insider (2018, marzo 16). *Digital Forensics Marke-Global Forecast to 2022*. Digital Forensics Market: https://markets.businessinsider.com/news/stocks/digital-forensics-market-global-forecast-to-2022-1018885400#

Moskvitch, K. (2013, julio 8). *Los adolescentes que ayudaron a ganar la Segunda Guerra Mundial*. Noticias: https://www.bbc.com/mundo/noticias/2013/07/130705_aficionados_radio_decodificadores_segunda_guerra_mundial_kv

Orozco, C. (2015, julio 25). Todo se puede monitorear. https://www.elespectador.com/entrevista-de-cecilia-orozco/todo-se-puede-monitorear-articulo-575035

Penlink. (2020). *Home*. https://www.penlink.com/

Pérez, G. (2016). *Hacking Team Malware para la vigilancia en América Latina*. Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

Privacity Internacional. (2015). *Un estado en la sombra: vigilancia y orden público en Colombia*. Privacity Internacional. https://privacyinternational.org/sites/default/files/2017-12/ShadowState_Espanol.pdf

Proyecto PV. (s.f.). *La red "Echelon"*. https://www.proyectopv.org/1-verdad/echelon.htm

Real Academia Española [RAE]. (2019). *Definición de interceptar.* https://dle.rae.es/interceptar

Real Decreto (1882, septiembre 14). Por el que se aprueba la Ley de Enjuiciamiento Criminal Ministerio de Gracia y Justicia [España]. https://www.boe.es/buscar/pdf/1882/BOE-A-1882-6036-consolidado.pdf

Resolución N.º 0-1037 (2016, abril 1). *Por la cual se reglamenta el funcionamiento del sistema de interceptación de las comunicaciones de la Fiscalía General de la Nación –SIC– se establece y organiza el departamento de interceptación de las comunicaciones –DIC–, adscrito a la Dirección de Fiscalías Nacionales, se determina su competencia y se dictan otras disposiciones*. Fiscalía General de la Nación [Colombia].

Resolución N.º 0020 de 2016 [Fiscalía General de la Nación] *Por medio de la cual se modifica la organización de la Dirección del Cuerpo Técnico de investigación y se dictan otras disposiciones*. Fiscalía General de la Nación [Colombia].

Rivera, J. C. & Rodríguez, K. (2015, mayo). *Vigilancia de las comunicaciones por la autoridad y protección de los derechos fundamentales en Colombia.* Electronic Frontier Foundation [EFF] & Comisión Colombiana de Juristas. https://www.eff.org/es/document/vigilancia-de-las-comunicaciones-por-la-autoridad-y-proteccion-de-los-derechos

Rodríguez, K. & Schoen, S. (2020, agosto 7). *FAQ: Why Brazil' s Plan to Mandate Traceability in Private Messaging Apps Will Break User' s Expectation of Privacy and Security.* https://www.eff.org/deeplinks/2020/08/faq-why-brazils-plan-mandate-traceability-private-messaging-apps-will-break-users

Salazar, C. (2014). El teletrófono, el celular y la literatura. *Revista Universidad de Antioquia* (315), 88-92.

Sánchez, J. (2016). *Estudio de la prueba electrónica en el proceso penal: especial referencia a las conversaciones de WhatsApp*. [Trabajo de Master en acceso a la Abogacía] Universidad de Salamanca. https://gredos.usal.es/handle/10366/132621

Sentencia C-566 (1995, noviembre 30) [Expediente N.º D-823] Magistrado Ponente: Eduardo Cifuentes Muñoz. Corte Constitucional [Colombia]. https://www.corteconstitucional.gov.co/relatoria/1995/C-566-95.htm

Sentencia C-586 (1995, diciembre 7) [Expediente N.º D-966] Magistrados Ponentes: Eduardo Cifuentes Muñoz y José Gregorio Hernández Galindo. Corte Constitucional [Colombia]. https://www.corteconstitucional.gov.co/relatoria/1995/C-586-95.htm

Sentencia C-336 (2007, mayo 7) [Expediente D-6473]. Magistrado Ponente: Jaime Córdoba Triviño. Corte Constitucional [Colombia]. https://www.corteconstitucional.gov.co/RELATORIA/2007/C-336-07.htm

Sentencia C-604 (2016, noviembre 2) [Expedientes acumulados D-11396 y D-11403] Magistrado Ponente: Luis Ernesto Vargas Silva. Corte Constitucional [Colombia]. https://www.corteconstitucional.gov.co/relatoria/2016/C-604-16.htm

Sentencia T-043 (2020, febrero 10) [Expediente T-7.461.559] Magistrado Ponente: José Fernando Reyes Cuartas. Corte Constitucional [Colombia]. https://www.corteconstitucional.gov.co/Relatoria/2020/T-043-20.htm

Sentencia (2012, noviembre 30) [Expediente 2010-0020]. Juzgado Tercero Penal del Circuotp Especializado de Descongestión de Bogotá, D. C. [Colombia]. http://www.derechos.org/nizkor/colombia/doc/das299.html#259.

Spyera. (2019). *Software de monitoreo para teléfonos móviles, tablets y computadoras.* https://spyera.com/es/

Supreme Justia. (1914). *Weeks v. United States, 232 U.S. 383 (1914).* https://supreme.justia.com/cases/federal/us/232/383/

Supreme Justia. (1928). *Olmstead v. United States, 277 U.S. 438 (1928).* https://supreme.justia.com/cases/federal/us/277/438/

Supreme Justia. (1967). *Katz v. United States, 389 U.S. 347 (1967).* Home: https://supreme.justia.com/cases/federal/us/389/347/

TICbeat. (2017). *¿Cuál es la diferencia: malware, virus, gusanos, spyware, troyanos, ransomware, etc?* https://www.ticbeat.com/seguridad/cual-es-la-diferencia-malware-virus-gusanos-spyware-troyanos-ransomware-etc/

Velásquez, F. (2021). *Fundamentos de Derecho penal. Parte general* (4ª ed.). Tirant lo Blanch.

United Kingdom (2016, noviembre 29). Investigatory Powers Act 2016. https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

Wainwright, T. (2016). *Narconomics. Cómo administrar un cártel de drogas*. Penguin Random House.

Winterman, D. (2014). *Los indígenas que dejaron perplejos a los alemanes en la Primera Guerra Mundial.* Noticias: https://www.bbc.com/mundo/noticias/2014/05/140521_cultura_codigos_guerra_finde_yv