REVISTA
CES DERECHO

ARTÍCULO DE INVESTIGACIÓN

Protección de datos personales recuperados en internet o dispositivos electrónicos en el proceso penal colombiano

Protection of personal data recovered on the internet or electronic devices in the colombian criminal process

Christian Camilo Gómez Gómez[1]

[1] Abogado universidad libre seccional Cúcuta, Docente en el área de derecho procesal de la universidad internacional del trópico americano, primer lugar concurso de ensayos en derecho internacional 2018. Candidato a magister en Derecho Procesal de la Universidad Libre.

Forma de citar: Gómez-Gómez, Christian Camilo. (2023). "Protección de datos personales recuperados en internet o dispositivos electrónicos en el proceso penal colombiano" En: *Revista CES Derecho*. Vol. 15. No. 1, enero a abril de 2024. pp. 17-30. https://dx.doi.org/10.21615/cesder.7236

Resumen
Esta investigación tiene como objeto de estudio el tratamiento de los datos personales en el proceso penal colombiano. Específicamente se analiza la diligencia del artículo 236 del código de procediendo penal, la recuperación de información dejada al navegar por internet en dispositivos electrónicos; se estudia la incidencia que tiene en la protección a la intimidad y privacidad de las personas, haciendo una crítica a las posiciones de la corte constitucional y corte suprema de justicia de lo que en la sociedad moderna se debe considerar, lo que es un teléfono celular y cómo en estos dispositivos electrónicos se pueden realizar hallazgos de datos personales.

Palabras clave: datos personales; teléfono celular; proceso penal colombiano.

Abstract
This investigation has as object of study the subject of the personal data in the Colombian criminal process the diligence of the article 236 code of penal procedure is analyzed, the information retrieval is allowed to browse the internet in the electronic devices, the incidence that the protection of privacy and privacy of people, protection of justice and privacy. Electronic devices can be made personal data findings

Keywords: personal data; cell phone; Colombian criminal process.

Introducción

La protección de los datos personales en Colombia surge con dos sistemas normativos la ley 1266 de 2008 que se encarga de regular el habeas data financiero y ley 1581 de 2012 que se encarga de regular la protección de los datos personales, la última será de especial importancia para el estudio de esta investigación ya que establece unas categorías especiales de los datos personales, como lo son los datos sensibles.

De otro lado, tenemos el proceso penal donde juega un papel fundamental el principio de legalidad, con la representación del juez de control de garantías para realizar el control de legalidad a las actuaciones que realiza la fiscalía en el procedimiento penal y así no afectar derechos fundamentales a los procesados.

Fecha correspondencia:
Recibido: 01 de marzo de 2023.
Revisado: 03 de noviembre de 2023.
Aceptado: 18 de enero de 2024.

DOI: 10.21615/cesder.7236
ISSNe: 2145-7719
https://revistas.ces.edu.co/index.php/derecho

A pesar de que la literata jurídica sobre la protección de los datos personales en el proceso penal en Colombia es poca, esta investigación pretende realizar una reflexión sobre la forma en la que debe realizarse cierta diligencia judicial ante la vulneración de derechos constitucionales, como lo son los datos personales.

Si bien el código de procedimiento penal colombiano establece ciertas diligencias que puede realizar el fiscal sin necesidad de un control de legalidad previo, como es el caso del art. 236 del C.P.P., siendo esta una actividad investigativa exenta de autorización judicial previa, actividad que alude a la recuperación de información cuando la evidencia relevante está contenida en un teléfono móvil y existen motivos razonados para concluir que el indiciado manipula a través de las redes de telecomunicaciones.

A diferencia de otras legislaciones, la colombiana expresa que estas actuaciones podrán hacerse solo con la autorización del fiscal, sin necesidad de un control jurisdiccional. En la normativa interna colombiana, el fiscal ordenara a la policía judicial la aprehensión de los dispositivos electrónicos y digitales para que un perito forense especialista en informática, analice la información recuperada y así obtenga evidencia para que se permita la captura del indiciado.

Aunque esta norma ha sido objeto de análisis por la corte constitucional y la corte suprema de justicia, para los altos tribunales, el escenario de abrir y examinar un dispositivo electrónico como el teléfono celular, no implica una interceptación, sino un simple registro de datos.

Ante este panorama el derecho a la tutela jurídica privada, el derecho a la intimidad y la privacidad no se afectan, no obstante, esta posición no parece ser acorde a las nuevas realidades tecnológicas que trascienden en la sociedad moderna de hoy en día.

Este postulado no es acorde a la realidad, el derecho como la realidad social se transforma y las normas deben adaptarse a ellas, máxime cuando estas son normas en las que derechos fundamentales como la intimidad y la privacidad se pueden ver afectadas, por interpretaciones no acordes a los tiempos que vivimos.

El celular es tal vez el dispositivo que más se usa en el mundo, con el auge de las redes sociales como, Facebook, Twitter e Instagram y las aplicaciones de mensajería como Whatssap, se hace necesario replantear las posturas jurídicas que algunos operadores jurídicos habían planteado antes, como es el caso objeto de la investigación, el celular más que un directorio de contactos se ha convertido en un dispositivo donde las personas incorporan fotos, videos, audios, conversaciones que tienen un alto contenido de datos personalísimos y que al trascender su contenido a terceros puede verse afectado el derecho a la intimidad y a la privacidad.

En opinión de esta investigación el control de legalidad que debe realizarse en esta diligencia debe ser de un control previo por parte del juez de control de garantías, es en estas situaciones en donde muchas veces el derecho encuentra confluencias cuando se encuentra con la tarea de entender y regular las nuevas tecnologías ya que estas innovaciones afectan algunos derechos fundamentales, para el caso que nos ocupa en esta investigación, este ensayo analizara aquellas vulneraciones a la protección de datos personales, al momento de adoptarse medidas jurídicas, para la obtención de información contenida en dispositivos digitales y electrónicos.

Con el fin de dar solución al problema jurídico que se plantea para el análisis de esta situación la investigación abordará: el concepto, las características y la clasificación de los datos personales a través de la ley, la jurisprudencia y la doctrina, seguidamente se estudiará la diligencia contenida en el art, 236 del código de procedimiento penal, el control de legalidad posterior y como es el desarrollo de la protección de datos personales en la recolección de las evidencias electrónicas, para posteriormente finalizar con las respectivas conclusiones.

Vol. 15 No. 1 / enero - abril de 2024

Descripción del problema de investigación

Actualmente en nuestra vida diaria la forma como más nos relacionamos es por sistemas digitales, gran parte de nuestro tiempo lo usamos en las redes, esta creciente interacción digital ha traído consigo múltiples conflictos en el estudio del derecho, por eso no es extraño que hoy los temas de gran relevancia para el estudio del derecho sean sobre evidencias digitales.

Ante lo cual surge el siguiente escenario en caso de vulneración a la protección de los datos personales en las diligencias de investigación penal:

Abrir y examinar un teléfono celular o computador, implicaría una intromisión a la privacidad o al acceso de información confidencial de la persona titular de esos datos personales, lo cual parecería que en este escenario jurídico se limita la protección del dato personal al momento de recolección y extracción de la evidencia digital.

El problema jurídico que se abordará en esta investigación será el siguiente: ¿Cuál es el procedimiento para la obtención de datos personales recuperados en internet y dispositivos electrónicos en el proceso penal en Colombia?

Objetivo

Analizar el procedimiento para la obtención de datos personales recuperados en internet y dispositivos electrónicos en el proceso penal en Colombia.

Metodología

El tipo de investigación es jurídica, de enfoque cualitativo porque se efectúa un estudio de carácter documental y descriptivo ya que está fundamentada en el análisis de las normas constitucionales, legales y referencias jurisprudenciales.

El método de investigación aplicado es la hermenéutica jurídica puesto que se basa en la interpretación sistemática del ordenamiento jurídico colombiano y en el análisis de los estudios del derecho. teniendo en cuenta que es una investigación de enfoque cualitativo no tiene un estudio de población y muestra, sino un estudio normativo.

Fuentes

Se utilizarán las principales fuentes del derecho como la constitución, ley, jurisprudencia y doctrina.

Resultados alcanzados

El dato personal y su protección

La importancia de los datos personales en las evidencias digitales ha tenido especial relevancia, el avance de las nuevas tecnologías y la incorporación de herramientas digitales implica que el tratamiento de datos personales sea un asunto de interés en cualquier área del derecho. Es importante para el desarrollo de esta investigación comenzar exponiendo algunos conceptos de dato:

> “Proveniente del latín datum que significa “lo que se da” es decir, un dato es toda información que se brinda, de manera alfabética, numérica, es una representación simbólica sobre hechos, elementos, etc. Ahora bien, cuando se habla de un dato personal se hace alusión a la información que permite individualizar e identificar a una persona como por ejemplo, su nombre, número de identificación, edad, número telefónico, información de salud, correo electrónico, dirección de residencia, información financiera, orientación sexual, política y religiosa, etc. (Hernández, 2018, pág. 9),

> El dato personal, tiene sus orígenes a partir de la interrelación con la privacidad, sin que puedan considerarse en el mismo contexto del mismo significante. Se debe tener en cuenta que existe mayor relación entre el derecho a la intimidad y la privacidad, que, entre el derecho a la protección del dato personal y la privacidad, no siendo presupuesto para establecer como función y finalidad de la privacidad, la protección del dato personal". (Elnecer, 2015, pág. 124).

En Colombia el art. 15 de la constitución política definió el derecho a la protección de datos personales en asocio con el derecho a la intimidad personal como derecho constitucional, y como tal es un derecho absoluto, imprescriptible, inalienable e inembargable, pudiendo cualquier ciudadano defenderlo frente a violaciones del estado, sus agentes y particulares.

Así la corte constitucional en sentencia, analiza la constitucionalidad de la ley estatutaria 1581 de 2012, afirmó que:

> "Toda persona por el hecho de serlo, es titular innato y exclusivo del derecho a la protección del dato personal, siendo el único legitimado a permitir la divulgación de sus datos personales concernientes a su vida privada, teniendo como finalidad, el aseguramiento de la protección de su Derecho Constitucional a que se le respete su intimidad, su buen nombre, su honra, en todo caso, los derechos morales de toda persona física en Colombia." (Corte Constitucional, Sentencia C-748 de 2011).

Es por ello que el titular de un dato personal, de acuerdo a la legislación colombiana actualmente, no permite que éste pueda renunciar total o parcialmente a su intimidad, toda vez que este acto jurídico estaría viciado de nulidad absoluta, estándar jurídico que servirá para analizar más adelante la situación de las redes sociales con sus cambios en políticas de privacidad, para con el tratamiento de datos personales de sus usuarios en el ciberespacio.

> "La protección del Dato Personal y la Intimidad, consagrada en el art. 15 de la C. Política, también se vincula al derecho a la autodeterminación informática "esta se enmarca en principios orientadores, que opera como parámetro para la validez de las actuaciones que adelantan las fuentes, operadores y usuarios del dato personal, así como fundamento para la exigibilidad jurídica de las facultades que se confieren al titular del dato." (Corte Constitucional, Sentencia C-748 de 2011).

Según la Definición dada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (artículo 3), y su Reglamento de desarrollo art. 5, partiendo de la definición que aporta la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos en su art. 2 Se entiende por dato de carácter personal.

Cualquier información concerniente a personas físicas identificadas o identificables. Una persona es identificable cuando su identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social, salvo que dicha identificación requiera actividades o plazos desproporcionados.

A la luz de esta definición los datos de carácter personal no se limitan únicamente a nombres y apellidos, sino que son una lista amplia y abierta, que va creciendo, y que incluye datos como nuestra voz, número de la seguridad social, nuestra dirección o datos económicos.

La Corte Constitucional en la sentencia señala las características de los datos personales:

> i) "estar referido a aspectos exclusivos y propios de una persona natural.

Vol. 15 No. 1 / enero - abril de 2024

ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos.

iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita.

iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación." (Corte Constitucional sentencia C-748,, 2011).

Hoy en día en Colombia, estos datos son almacenados de diversas maneras, como por ejemplo de forma "no automatizada", esto es, datos que se encuentren almacenados en medios físicos, como archivos, fichas de pedido de proveedores, hojas de vida físicas, un cuaderno, etc. o también de manera "automatizada", es decir almacenada en medios informáticos o virtuales, bien sea por personas naturales o jurídicas, públicas o privadas. Debido a las diferentes formas en que son almacenados los datos personales es que surge la importancia de clasificarlos y darles una categoría a cada uno ya que según el tipo de dato será el grado de protección, es por ello que la ley es clara en garantizar esa protección y lo que pretende es establecerle a los responsables del almacenamiento, es decir, las entidades públicas o privadas, personas naturales o empresas comerciales, exigiéndoles unas medidas de seguridad dependiendo del tipo de dato del que se trate, esto con la finalidad de evitar posibles sanciones." (Hernández, 2015, pág. 10).

La Ley 1266 de 2008 trae una categorización de los datos personales, clasificándolos en "datos privados" "datos semiprivados" y "datos públicos", además, la Ley 1581 de 2012 consagra unas categorías especiales de los datos personales, denominándolos "Datos sensibles" y "datos personales de los niños, niñas y adolescentes", entonces, actualmente los datos en Colombia se clasifican en, "datos personales" "datos públicos" "datos privados" dato semiprivados", "datos sensibles" y " datos de niños, niñas y adolescentes".

Para efectos de esta investigación estudiaremos los datos sensibles a los cuales puede acceder el perito forense en la diligencia de recuperación de información en dispositivos electrónicos.

El dato sensible

Los datos sensibles son aquellos que pertenecen a una categoría de especial protección por la ley, debido a que su contenido puede afectar el derecho a la privacidad, generándose discriminación y afectado su dignidad humana. La ley 1581 de 2012 establece que estos datos están ligados a la esencia intima de las personas y que su exposición puede generar situaciones de discriminación, no pueden ser objeto de tratamiento a menos que sea requerido para salvaguardar un interés vital del titular o este se encuentre incapacitado y su obtención haya sido autorizada expresamente.

De manera general, se consideran datos sensibles aquellos que revelan características como origen étnico o racial, datos de salud, preferencia sexual, filiación política, religión, ideología, afiliación a sindicatos, organizaciones sociales, datos biométricos, entre otros. Es por esto que esta clase de información debe ser tratada con mayor responsabilidad. Los datos de los niños, niñas y adolescentes también forman parte de esta categoría.

Estructura de la diligencia para la obtención de datos personales en internet o dispositivos electrónicos

La diligencia de investigación realizada para la obtención de información contenida en internet o aparatos electrónicos, se realiza de la siguiente forma:

"Esta audiencia supone un control constitucional posterior a las actuaciones realizadas por la Fiscalía

> General de la Nación, en torno al cumplimiento de la orden de registro y allanamiento. De gran importancia resulta en este punto de la investigación, analizar la audiencia de control de legalidad posterior a las órdenes de registro y allanamiento.
>
> Dentro de las veinticuatro (24) horas siguientes al recibimiento del informe de Policía Judicial sobre las diligencias de las órdenes de registro y allanamiento, retención de correspondencia, interceptación de comunicaciones o recuperación de información producto de la transmisión de datos a través de las redes de comunicaciones, el fiscal comparecerá ante el Juez de Control de Garantías, para que realice la audiencia de revisión de legalidad sobre lo actuado.
>
> Durante el trámite de la audiencia podrán asistir, además del fiscal, los funcionarios de la Policía Judicial y los testigos o peritos que prestaron declaraciones juradas con el fin de obtener la orden respectiva, o que intervinieron en la diligencia.
>
> El juez podrá, si lo estima conveniente, interrogar directamente a los comparecientes y, después de escuchar los argumentos del fiscal, decidirá de plano sobre la validez del procedimiento.
>
> El objeto principal de la audiencia es que el Juez de Control de Garantías revise formal y materialmente la orden de la diligencia y el procedimiento de allanamiento y registro." (Congreso de la República, Ley 906 de 2004).

Para la audiencia que enuncia el artículo 236 del código de procedimiento penal, para la recuperación de información dejada al navegar por Internet u otros medios tecnológicos que produzcan efectos equivalentes, se realiza un control de legalidad posterior ante el juez de control de garantías, situación que no encontramos acorde a la protección de derechos constitucionales como el de los datos personales, por la siguiente razón:

> "Al momento que el experto forense especialista en informática, realice el examen del teléfono celular, encontrara fotos, videos, conversaciones que pueden revelar la ideología política, la orientación sexual y religiosa de la persona, situación que afecta el derecho a la intimidad de las personas. La intervención de un teléfono celular, además de necesaria, razonable y proporcional, ha de tomar en consideración las siguientes circunstancias: que es una medida excepcional y no procede cuando exista otra de menor incidencia; que su finalidad es exclusivamente probatoria y solo se aplica para delitos graves; que debe mediar autorización judicial motivada; que son arbitrarias las intervenciones exploratorias; que solo es posible intervenir el teléfono del indiciado o inculpado y que se impone la revisión posterior por parte del juez de garantías con la asistencia del imputado y su defensor para que ejerzan el contradictorio, si lo desean. " (Fernandez Leon, 2017).

Esta situación genera una afectación a los datos personales de la persona que está siendo objeto de investigación penal, los datos sensibles al tener una categoría de especial protección deberían tener un tratamiento distinto al que actualmente la ley establece con el fin de no afectar el derecho a la intimidad y la dignidad del titular de los datos sensibles.

La protección de los datos personales en el procedimiento de recolección en internet o dispositivos electrónicos en el proceso penal colombiano

Tal vez el dispositivo electrónico más usado en el mundo sea el Teléfono celular, una mezcla entre un aparato electrónico inteligente y un ordenador de bolsillo, en el cual se guarda una agenda de contactos, fotos, videos, Audios, correos electrónicos enviados y recibidos, además con el desarrollo de las tecnologías, hoy en día, el uso del celular con aplicaciones de mensajería como WhatsApp o redes sociales como Instagram y Facebook, implica que estos dispositivos contienen Datos personales, que en algunos casos acceder a ellos implicarían una intromisión a información que hace parte de la privacidad de las personas.

Vol. 15 No. 1 / enero - abril de 2024

Aquí presta especial atención el primer escenario de estudio en esta investigación, abrir y examinar un teléfono celular, computador o perfiles de redes sociales, implicaría una intromisión a la privacidad o al acceso de información confidencial de la persona titular de esos datos personales.

La legislación en materia penal en Colombia dispone una entre las actividades investigativas exentas de autorización judicial previa para su realización, el artículo 236 del Código de Procedimiento Penal alude a la "recuperación de información", medida pertinente cuando la evidencia relevante está contenida en un teléfono móvil y existen motivos razonablemente fundados para inferir que el sospechoso transmite o manipula datos a través de las redes de telecomunicaciones.

> "Artículo 236. recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes: Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o el imputado está transmitiendo o manipulando datos a través de las redes de telecomunicaciones, ordenará a policía judicial la retención, aprehensión o recuperación de dicha información, equipos terminales, dispositivos o servidores que pueda haber utilizado cualquier medio de almacenamiento físico o virtual, análogo o digital, para que expertos en informática forense, descubran, recojan, analicen y custodien la información que recuperen; lo anterior con el fin de obtener elementos materiales probatorios y evidencia física o realizar la captura del indiciado, imputado o condenado. En estos casos serán aplicables analógicamente, según la naturaleza de este acto, los criterios establecidos para los registros y allanamientos."

La aprehensión de que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida. Inmediatamente se devolverán los equipos incautados."

> A diferencia de otras legislaciones, en Colombia la normativa ampara estas actuaciones con la sola orden del fiscal, en el entendido de que abrir y examinar un celular no implica que se está realizando interceptaciones , sino un intranscendente registro de datos, siguiendo estas líneas las altas cortes en Colombia han entendido que la información que pueda aparecer contenida en el disco duro y en el teléfono, no es necesariamente una base de datos personales y como consecuencia no hay necesidad de un control previo por parte del juez de control de garantías. (Fernández, 2017).

Situación que no es la más adecuada para la protección de los datos personales y el derecho a la intimidad, el control previo por parte del juez de control de garantías en el ámbito penal se establece con el fin de:

> "En el caso del control previo, procede una actuación judicial que pondera entre los intereses de la investigación, las razones aducidas por la Fiscalía, el delito investigado y las condiciones del sujeto sobre quién o sobre cuyos intereses se practicaría la actuación, a fin de evitar una restricción excesiva, innecesaria o afrentosa, que en poco o nada asegure verdad al proceso y al contrario, afecte desproporcionadamente ámbitos de la intimidad y privacidad de la persona implicada. Lo que hace el juez es proteger los derechos del sujeto investigado, impedir que las prerrogativas del Estado asignadas a la Fiscalía y a su aparato técnico, se usen sin finalidad concreta, sin justificación, inútilmente y de modo desproporcionado, desconociendo el carácter iusfundamental y especialmente protegido de los bienes jurídicos reconocidos en los derechos individuales sobre los que la actuación investigativa opera". (Corte Constitucional, Sentencia C 334 de 2010).

Pareciera existir entonces un contrasentido entre el fin del control previo judicial realizado por el juez de control de garantías y la actuación de la fiscalía al momento de obtener la evidencia digital, con la actividad exenta de control previo, como lo es la recuperación de información contenido en dispositivos digitales.

Los desarrollos en las nuevas tecnologías, los ciberataques, formas de suplantación de identidad, los mensajes por WhatsApp de perfiles y números falsos para apropiarse de datos financieros, muestran que la ley luce

rezagada e insuficiente. Actualmente la interacción digital ha crecido exponencialmente y después de la pandemia el mundo se vio obligado a usar aún más los avances tecnológicos para estar comunicados, uno de esas herramientas es el teléfono celular, que ya no se reduce solo a una libreta de direcciones de contactos, para las personas el celular es una extensión de su trabajo y de su vida personal, que contiene información muy valiosa alguna íntima y confidencial, por lo que conserva una expectativa razonable de que esos contenidos no trasciendan a terceros.

No obstante, cuando estas herramientas son analizada por expertos forenses designados para extraer la información y al efectuar el backup se recuperaran los contactos, las llamadas recibidas, las marcaciones, los datos acopiados en la memoria, pero también hará descubrimientos fortuitos y reservados, el perito forense podrá acceder a conversaciones de whatssap, Facebook, Instagram, donde tendrá acceso a una amplia galería de fotos , videos, mensajes de voz y muchas otras cosas intimas, lo que implica una vulneración de los derechos a la intimidad y a la tutela jurídica de la vida privada.

No obstante, los pronunciamientos de la jurisprudencia han establecido una línea de pensamiento que distorsiona lo que es la protección de datos personales en la evidencia digital, en esta línea de pensamiento, la Corte Suprema de Justicia señaló:

> “Resulta inconsecuente creer que revisar la información contenida en un teléfono celular, implica intromisión a la privacidad o el acceso a información confidencial (…) nadie ha dicho que el teléfono celular contiene información organizada a manera de bases de datos. Lo que existe en el celular es un simple sistema de información creado por el usuario.” (Corte Suprema de Justicia Sentencia de Casación Penal nº 29991 de 2008).

La Corte Constitucional también ha señalado que:

> “La información que pueda aparecer en el disco duro y en el teléfono celular de un sujeto investigado no es necesariamente una base de datos.” (Corte Constitucional, Sentencia C 334 de 2010).

En fallos recientes, añadió que monitorear la información guardada en el celular no conlleva intromisión de alta intensidad en la órbita privada de la persona, ya que aquella es equiparable a un documento digital cuya extracción pueden realizar fiscalía o defensa como acto investigativo propio, siempre que aparezca necesario, razonable y proporcional.

Situación que parece contraria a lo que ha establecido la corte en fallos anteriores donde estipulaba que:

> “Finalmente, encontramos la información reservada, que por versar igualmente sobre información personal y sobre todo por su estrecha relación con los derechos fundamentales del titular - dignidad, intimidad y libertad- se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones. Cabría mencionar aquí la información genética, y los llamados "datos sensibles" o relacionados con la ideología, la inclinación sexual, los hábitos de la persona, etc.” (Corte Constitucional, Sentencia T 114 de 2018).

Lo que significa que los datos personales contenidos en teléfonos celulares como fotos, videos, audios, whatsapps, no pueden ser obtenidos o examinados por parte de un equipo forense digital, a menos que exista un control previo por parte del juez e control de garantías, ya que muy posiblemente pueden existir violaciones a derechos fundamentales.

Al abrir o acceder a tales medios, no se sabe si en ellos reposa información confidencial, posibilidad que tiene entonces que “legalizar el Juez de Control de Garantías”. En el escenario internacional, en razón de los diferentes tratados de derechos humanos, se hace un especial reconocimiento al derecho a la protección de datos; de allí

Vol. 15 No. 1 / enero - abril de 2024

la necesidad de actuar con mayor "prudencia judicial", para no incurrir en investigaciones de la Comisión Interamericana de Derechos humanos.

> "En esta línea destaca apartes de la observación general No. 16, sobre el art. 17 del PIDCP, elaborada por el Comité de Derechos Humanos, en el que se llama a los Estados a adoptar medidas para que la información relativa a la vida privada de una persona, no caiga en manos de personas no autorizadas por la ley, ni sea utilizada con fines incompatibles con el Pacto." (observación general N. 16, 2005).

El control previo de garantías en la protección de datos personales en las investigaciones judiciales

El control previo de garantías es una forma legalidad para evitar posibles anulaciones de actuaciones judiciales que sean violatorias a derechos fundamentales es por ello que un juez diferente al que juzgara se encarga de esta tarea.

A partir de la expedición del Acto Legislativo 03 de 2002, se reconfigura el Sistema Procesal Penal, en tal sentido las partes e intervinientes asumen nuevos roles, características y funciones, es por ello que la Fiscalía se desprende de la total discrecionalidad para afectar los derechos de las personas de la que gozaba bajo el sistema mixto. Dentro del nuevo esquema la Fiscalía tiene la posibilidad de emitir órdenes para ejecutar determinadas diligencias, con el deber de someterlas a un Control posterior ante el Juez con funciones de Control de Garantías, para que él resuelva sobre su legalidad formal y material, de tal suerte que si el Juez en su análisis determina la existencia de irregularidades en la orden o en su diligenciamiento, sobre los Elementos Materiales Probatorios y Evidencia Física recolectados en desarrollo de referidas órdenes recae la denominada Cláusula de Exclusión. Entre las actuaciones ejecutadas por la Policía Judicial que requieren orden previa del Fiscal y control Posterior del Juez de Garantías, se cuentan la recuperación de información dejada al navegar por Internet. (Daza, 2007).

> "La cláusula de exclusión mencionada sobre una prueba obtenida de manera directa en virtud de la violación de un derecho fundamental, o derivada de ella se da por: i) deterrent effect (efecto disuasivo) y ii) tutela de los derechos constitucionales fundamentales. En principio estas finalidades no son excluyentes, sin embargo, dependiendo de cuál se tome como prevaleciente, se edificarán diferentes criterios de admisibilidad probatoria excepcional de prueba ilícita." (Sanabria, 2014).

No obstante, este artículo de investigación ha criticado la postura que adoptó el órgano legislativo y la interpretación de las altas cortes con respecto a la valoración de los teléfonos celulares y del PC en relación a los datos personales.

En esta diligencia el Fiscal puede ordenar la recuperación de la información trasmitida por el indiciado a través de Internet u otros medios tecnológicos, siempre que tenga motivos razonablemente fundados, basado en los medios cognoscitivos previstos en la Ley, a partir de los cuales se pueda inferir que, a través del uso de dichos elementos, el indiciado ha manejado información útil para la investigación que se adelanta.

El Fiscal ordena la aprehensión de los computadores y servidores que pueda haber utilizado, disquetes y demás medios de almacenamiento físico, para que expertos en informática forense descubran, recojan, analicen y custodien la información que recuperen.

La regla general para el ejercicio del juez de control de garantías de un control previo es que la actuación o las medidas afecten derechos fundamentales y en este caso la diligencia de recuperación de información dejada al navegar en internet y otros medios similares, pueden ser susceptibles de violaciones, independientemente de que a través de medios electrónicos se pueda estar consumando una conducta punible, pues el acceso a la memoria RAM, disco duro o dispositivos de almacenamiento masivo podría afectar el derecho a la intimidad sin contar con el control previo del juez de control de garantías.

Para ilustrar un ejemplo de cómo puede afectarse la intimidad, imagínese que la fiscalía incauta su Pc y celular, en ellos se encuentran datos como historia clínica, fichas de actos religiosos, fotos y vides con su pareja, etc, datos que han sido clasificados por la doctrina, la jurisprudencia internacional y organismos de derechos humanos como "sensibles". Una categoría que proviene de la Constitución, en concordancia con la Declaración de Derechos Humanos.

No puede existir entonces una legalización sobre la apertura de los ficheros digitales en una investigación penal con el pretexto de la urgencia cuando se pueden violar datos sensibles, al ser posterior el control de garantías y no previo, el fichero queda modificado desde el momento en que se abre. Y aunque exista seguridad de que el forense no realizó ninguna operación, en todo caso se crea lo que se conoce como una nueva "huella de hash". En consecuencia, la Audiencia de Control de Garantía no puede ser después de abierto los documentos. Para ello tienen que haberse tomado sus "metadatos" y la huella hash, y luego, con la autorización del juez de control de garantías, el perito forense podrá realizar el análisis de la información.

En estos casos para que el documento electrónico quede inalterable, el perito forense realizara copias espejo o la aplicación del proceso informático "imaging", técnicas mediante las cuales se obtienen copias exactas del disco duro de un equipo electrónico o de un soporte de almacenamiento digital, esto para que en el momento de la cadena de custodia se pueda asegurar la evidencia digital y así evitar un mal uso de la recolección de evidencia digital, tal y como sucedió con el caso de Raúl Reyes con los dispositivos electrónicos, rompiéndose la cadena de custodia para posteriormente realizar el análisis forense.

Esta es una de las razones que sustentan que el control de garantías deba operar de forma previa a la intervención forense, porque así se desprende del art. 250 numeral 3º CP, donde se obliga a acudir al juez de control de garantías "cuando se vulneran derechos fundamentales, como ocurría en el caso en estudio, con el derecho a la intimidad, pues la revisión del disco duro y del teléfono celular puede arrojar el acceso a información reservada.

En el caso de haber encontrado y accedido a archivos relacionados con aspectos de la intimidad de la persona, como datos sensibles, se violaría el derecho a la intimidad, pero también se pondría en duda la inalterabilidad, autenticidad y conservación de los datos.

Al no estar asegurado el cumplimiento de protocolos de manejo de la cadena de custodia sobre evidencias digitales y al existir sólo un control de legalidad posterior ante el juez de garantías, no se asegura que tal información allegada al proceso sea confiable.

Pues esta evidencia no deberá ser puesta al control de juez de garantías después de 24 horas de recolectada sino antes, cuando su captura y cadena de custodia ha sido lograda por la Policía Judicial, para luego sí, con la anuencia del Juez Constitucional, se logre acceder a todos los ficheros sin importar la clasificación de la información, en aras de encontrar más información.

La información que pueda aparecer en el disco duro y en el teléfono celular de un sujeto investigado no es necesariamente una base de datos. Este es el planteamiento que uso el alto tribunal para la negación de la pretensión de la inconstitucionalidad de la norma demandada.

Sin embargo, al abrir o acceder a tales medios, no se sabe si en ellos reposa información confidencial, posibilidad que tiene entonces que "legalizar el Juez de Control de Garantías". Y es en esa línea, que, en el escenario internacional, en razón de los diferentes tratados de derechos humanos, se hace un especial reconocimiento al derecho a la protección de datos; de allí la necesidad de actuar con mayor "prudencia judicial", para no incurrir en investigaciones de la Comisión Interamericana de Derechos humanos.

"En esta línea destaca apartes de la observación general No. 16, sobre el art. 17 del PIDCP, elaborada por el

Vol. 15 No. 1 / enero - abril de 2024

Comité de Derechos Humanos, en el que se llama a los Estados a adoptar medidas para que la información relativa a la vida privada de una persona, no caiga en manos de personas no autorizadas por la ley, ni sea utilizada con fines incompatibles con el Pacto." (Observación General N. 16, 2005).

El hecho que una autoridad judicial revise la constitucionalidad de la revisión, de unos dispositivos donde posiblemente se guarden datos personales y se colija la inalterabilidad de la evidencia, es darle más y mejores garantías al ciudadano sub judice.

De lo anterior concluyen que es necesario el control previo de las diligencias por parte del juez de control de garantías, como forma de establecer límites para la intervención sobre derechos fundamentales.

Así que el control de legalidad debe ser previo para evitar excesos, ya que el control posterior no restablece de ninguna manera derechos conculcados, pues no los devuelve a su estado anterior. Además, con el control previo se evitan excesos y se determinan los límites de la actuación sobre los derechos fundamentales, así como quién es el encargado de hacer dicha intervención para los efectos del control de la cadena de custodia.

La informática forense en el proceso penal

Hoy, en la mayoría de los procesos judiciales, se involucra la evidencia digital. Tras los casos de fraudes empresariales, robos a empresas, casos de competencia desleal, hurtos virtuales, secuestros y extorsiones a empresarios, entre otras graves conductas, los servicios de investigación forenses y probatorios ofrecen una respuesta ágil para brindar soporte técnico y jurídico en investigaciones de este tipo de fraudes.

Actualmente, la labor de los abogados es insuficiente, si no está acompañada de procesos técnicos probatorios confiables.

> "Un abogado con un Código Civil y la Constitución encima del escritorio no hace nada. Debe tener un grupo grandísimo de expertos. Detrás de un fiscal, hay un investigador, policía judicial y toda la tecnología del mundo. Por eso, ese abogado tiene que rodearse de un equipo forense profesional", esto es lo que señalan expertos en investigación forense.
>
> Así las cosas, la ciencia forense y las nuevas herramientas tecnológicas hoy juegan un papel decisivo en los procesos judiciales. La llamada prueba pericial es uno de los elementos más importantes que tiene en cuenta un juez al tomar una decisión.
>
> De esta manera, los abogados, jueces o fiscales son conscientes de que muchas evidencias, pruebas y notificaciones en los procesos administrativos y judiciales están soportadas en correos electrónicos, grabaciones, mensajes de texto, páginas de internet, entre otros. Por esa razón, es indispensable que los profesionales del Derecho, sin importar su rol, conozcan las normas legales que se deben adecuar a las exigencias técnicas, de conformidad con los tipos de prueba propios que exige cada proceso". (Ambito Juridico, 2013).

Debido al desarrollo de lo evidencia digital es que se hace necesario promover por el desarrollo de un "estándar legal de políticas de seguridad informática", que habilite la admisibilidad de pruebas de tal naturaleza, esto es su presunción *iuris tantum* de validez como evidencia digital.

La prueba dentro del proceso penal es de especial importancia, ya que desde ella se confirma o desvirtúa una hipótesis o afirmación precedente, se llega a la posesión de la verdad material.

> "De esta manera se confirmará la existencia de la infracción y la responsabilidad de quienes aparecen en un inicio como presuntos responsables, todo esto servirá para que el Tribunal de Justicia alcance el

> conocimiento necesario y resuelva el asunto sometido a su conocimiento. El objetivo de la Informática forense es el de recobrar los registros y mensajes de datos existentes dentro de un equipo informático, de tal manera que toda esa información digital, pueda ser usada como prueba ante un tribunal". (Acurio Del Pino, 2009).

Ahora en el marco de todo proceso judicial, al examinar evidencias digitales contenidas en teléfonos celulares, el perito forense no solo tendrá acceso a datos sensibles de la persona dueña del celular, sino también de terceros que no se relacionen con el proceso penal pero que vayan tenida interacción digital por medio de redes sociales.

La cadena de custodia informático- forense

La cadena de custodia tiene como finalidad brindarle soporte veraz a la prueba digital ante el juez, en medio de lo que se conoce como el debido proceso. Por tal motivo deben establecerse los procedimientos indicados para garantizar la idoneidad de los métodos aplicados para la sustracción de la evidencia informática. Así se garantiza una base efectiva para el juzgamiento y la validez ante cualquier fuero judicial internacional. Para esto, es necesario que se eviten suplantaciones, modificaciones, alteraciones, adulteraciones o simplemente su destrucción (común en la evidencia digital, ya sea mediante borrado o denegación de servicio). Procedimiento controlado y supervisable, la cadena de custodia informático-forense se aplica a los indicios materiales o virtuales relacionados con un hecho delictivo o no, desde su localización hasta su Valoración por los encargados de administrar justicia.

> "La preservación de la cadena de custodia sobre la prueba indiciaria criminalística es obligación de la totalidad de los miembros del poder judicial, los operadores del derecho y sus auxiliares directos. Entre estos últimos debemos incluir el personal de las fuerzas de seguridad, la policía judicial y el conjunto de peritos oficiales, de oficio y consultores técnicos o peritos de parte. Así, la implementación de mecanismos efectivos de recopilación de evidencias debe incluir procedimientos que aseguren la confiabilidad de la información recolectada. Dicha confiabilidad incluye la trazabilidad, (Establecer un mecanismo que permita realizar un seguimiento estricto de los elementos probatorios, desde su detección hasta el momento de su disposición definitiva) la confidencialidad, la autenticidad, la integridad y el no repudio de los datos. En términos sencillos, implica establecer mecanismos de garantía de que los elementos probatorios ofrecidos como prueba documental informática son confiables, es decir, que no han sufrido alteración o adulteración alguna desde su recolección". (Arellano & Castañeda, 2012).

Procedimiento para la obtención de datos personales recuperados en internet y dispositivos electrónicos en el derecho comparado

En el proceso Penal Estadounidense el papel de los jueces en la investigación de los delitos es limitado. Sin embargo, ciertas acciones durante una investigación sólo pueden llevarse a cabo con la autorización de un juez. Solamente un juez puede dictar una orden de cateo e incautación de pruebas de delitos; solamente un juez puede ordenar la grabación de conversaciones telefónicas; solamente un juez puede tomar medidas para obligar a cumplir una orden de comparecencia (una orden de que un testigo rinda testimonio o presente documentos u otras pruebas que obren en su poder, bajo pena de privación de la libertad si se niega a hacerlo); y, excepto en circunstancias limitadas, solamente un juez puede dictar orden de arresto contra una persona acusada.

> "Siempre que un fiscal (o, en algunos casos, un policía) determina que se requiere este tipo de acción judicial en una investigación, presenta una solicitud formal ante el tribunal y plantea hechos o pruebas legalmente suficientes para apoyar la acción solicitada. Un juez dicta la orden solicitada solamente si determina que existen bases de hecho suficientes para hacerlo. Por ejemplo, en el caso de una solicitud de orden de cateo, el tribunal debe determinar que las pruebas presentadas son suficientes para establecer causa probable para creer que se ha cometido un delito y que pueden encontrarse pruebas de

Vol. 15 No. 1 / enero - abril de 2024

> dicho delito en un sitio específico que será cateado.” (Organizacion de Estados Americanos, 2018)
>
> “Por lo tanto se protege a los ciudadanos de los registros e incautaciones irrazonables e impone la obligación de expedir orden judicial para efectuar el registro o la incautación, siempre que exista causa probable” (Lexbase Colombia, 2012).

En España esta situación ha sido analizada por el tribunal constitucional en la STC 173/2011, 7 de noviembre, recuerda la importancia de dispensar protección constitucional al cúmulo de información personal derivada del uso de los instrumentos tecnológicos de nueva generación. Lo que se está definiendo es un nuevo derecho fundamental basado en la consideración de estos instrumentos como lugar de almacenamiento de una serie compleja de datos que afectan de modo muy variado a la intimidad del investigado (comunicaciones a través de sistemas de mensajería, por ejemplo, tuteladas por el art 18 3º CE , contactos o fotografías, por ejemplo, tuteladas por el art 18 1º CE que garantiza el derecho a la intimidad, datos personales y de geolocalización, que pueden estar tutelados por el derecho a la protección de datos, artículo 18 4º CE). (García, 2017).

Allí puede leerse el siguiente razonamiento:

> “Si no hay duda de que los datos personales relativos a una persona individualmente considerados, a que se ha hecho referencia anteriormente, están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) -por lo que sus funciones podrían equipararse a los de una agenda electrónica-, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona”. (Tribunal Constitucional de España, Sentencia 173, 2011).

Es decir que el tribunal reconoce que al momento de analizarse un ordenador se podrán encontrar fotos, videos, chats, ya que por medio de ellos las personas descargan imágenes, videos y almacenan conversaciones, lo que muestra aspectos íntimos de la personalidad de cada ser humano, lo que hace que sean datos personales de especial protección, como lo son las preferencias sexuales, la ideología política, información sobre la salud, creencias religiosas, etc.

Conclusiones

La obtención de la evidencia digital en Colombia como es el caso de la obtención de recuperación de información dejada en internet, como lo son los celulares, debe ser objeto de un control previo por parte del juez de control de garantías, pues estos medios digitales pueden contener datos personales sensibles.

La intervención de un teléfono celular además de ser una medida tomada en razón a la necesidad, proporcionalidad y razonabilidad, debe ser una medida excepcional y no debe proceder si existen otras medidas de menor incidencia, su finalidad debe ser probatoria y solo debe aplicarse a delitos muy graves, la autorización judicial debe ser motivada, no pueden realizarse solo con fines exploratorios y cuando se obtenga el materia

probatorio o la evidencia contenida en medios electrónicos, debe contarse con la asistencia del imputado con su abogado defensor para que ejerza el contradictorio.

Las nuevas tecnologías llevan consigo cambios y uno de estos es el cambio en las posturas jurídicas y en la ley, el derecho debe seguir los pasos de las innovaciones tecnológicas, en el campo de la protección de datos se hace necesario estar a la vanguardia de las nuevas tendencias internacionales, no se trata de enfrentar el desarrollo digital con el derecho, sino de pintar nuevos senderos, como lo afirma el tratadista Ernesto Benda: tan pronto como se opta por un determinado camino, aparecen nuevos senderos que obliga a decidir sobre el itinerario.

Referencias

Acurio Del Pino, S. (2009). Manual de Manejo de Evidencias Digitales y Entornos. *fiscalia general del Estado de Ecuador*, pags. 1-18. dipsonible en: Manual de Manejo de Evidencias Digitales y Entornos Informáticos (alfa-redi.org)

Ámbito Juridico. (05 de agosto de 2013). Tecnología en el proceso judicial, una herramienta al servicio del Derecho. *Ambito Juridico*, pág. 2 obtenido de: Tecnología en el proceso judicial, una herramienta al servicio del Derecho | Ámbito Jurídico (ambitojuridico.com)

Manual De Peritaje Informatico. Maricarmen Pascale, Fundación de Cultura Universitaria. Uruguay. 2007.

Arellano, l. e., & Castañeda, C. M. (2012). La cadena de custodia informático-forense. *Revista ACTIVA*, pp.67-81.

Daza González, A. (2007). "Actuaciones de la policía judicial que requieren orden del fiscal y control judicial posterior". En: *Prolegómenos - Derechos y Valores Volumen X - Nº 20*, 137-148.

Elnecer Mesa, A. M. (2015). la evidencia digital eximiente de violación a la protección del dato personal. *Academia & Derecho, (10)*, 119-156, https://doi.org/10.18041/2215-8944/academia.10.351.

Fernández Leon, W. (23 de marzo de 2017). La recuperación judicial de información almacenada en celulares. *Ambito Juridico* , pág. 3. obtenido de: La recuperación judicial de información almacenada en celulares | Ámbito Jurídico (ambitojuridico.com)

García Borrego, J. A. (2017). *Análisis de la regulación y jurisprudencia actual de las Diligencias de Investigación en el Proceso Penal y la actuación de la Policía Judicial, en particular, la intervención de las nuevas modalidades de comunicaciones personales.* Murcia: universidad catolica de murcia.

Hernández Lotero, N. (2018). *Clasificación de los datos personales e implicaciones legales.(trabajo de grado)* medellin: Universidad Pontificia Bolivariana. obtenido de: Clasificación de los datos personales e implicaciones legales (upb.edu.co)

Introducción A La Informática Forense. Dr. Santiago Acurio Del Pino, Director Nacional De Tecnologías De La Información De La Fiscalía General Del Estado. pags. 1-33, obtenido de : Informática Forense en el Ecuador (alfa-redi.org)

Lexbase Colombia. (4 de abril de 2012). *La Regla de Exclusión.* Obtenido de tendencias Lexbase: http://blogs.portafolio.co/juridica/la-regla-de-exclusion/

Organización de Estados Americanos (2018), *Guía sobre los procesos penales en los Estados Unidos*, Obtenido de: http://ru.juridicas.unam.mx/xmlui/handle/123456789/2355

Sanabria Villamizar, R. J. (Julio-Diciembre de 2014). Teleología de la cláusula de exclusión en Colombia. Revista Academia & Derecho, 5(9), (83-110) obtenido de: Teleología de la cláusula de exclusión en Colombia - Dialnet (unirioja.es)

Corte Constitucional. Sentencia 173, BOE núm. 294 (tribunall consititucional de España 7 de noviembre de 2011).

Corte Constitucional. Sentencia C-334, expediente D-7915, corte constitucional - 12 de mayo de 2010 - . M.P. Juan Carlos Henao Perez, obtenido de: https://www.corteconstitucional.gov.co/relatoria/2010/C-334-10.htm

Corte Constitucional. Sentencia C-748, expediente PE-032,Corte constitucional M.P. Jorge Ignacio Pretel Chalbuj 06 de octubre de 2011 disponible en: https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm.

Corte Suprema de Justicia. Sentencia de Casación Penal nº 29991, Proceso No. 29991 (Corte Suprema de justicia 2 de julio de 2008).

Corte Suprema de Justicia. Sentencia T-114 , Expediente T-6.492.167 (Corte Constitucional, M.P. Carlos Bernal Pulido 03 De Abril De 2018).

Department of Home and Land Security and The United States Secret Service. *The Best Practices For Seizing Electronic Evidence*, Versión 3.0, Us.