

TRATAMIENTO DE DATOS PERSONALES EN EL PROCESO PENAL COLOMBIANO. TÉCNICA JUDICIAL

BÚSQUEDA SELECTIVA EN FICHEROS TELEFÓNICOS

Por Alexander Díaz García

Nuestra Corte Constitucional¹, se ha referido que el interés de la sociedad en que se investiguen las conductas delictivas y se sancione a sus responsables, en procura de preservar la vigencia de un orden justo, es también un bien protegido por la Constitución. En su sentencia se refiere que el acopio de información en relación con las personas puede ser eventualmente un medio necesario para la satisfacción de ese interés constitucionalmente protegido. Sin embargo, su recaudo debe realizarse con escrupuloso acatamiento de las cautelas que la propia Constitución ha establecido para la protección de los derechos fundamentales especialmente expuestos a su afectación, vulneración o mengua en el contexto de una investigación criminal.

El requerimiento de autorización judicial previa para la adopción de medidas –adicionales- que implique afectación de derechos fundamentales es una de esas cautelas que el legislador debe acatar al configurar las reglas orientadas a regular la actividad investigativa del Estado. Agrega que la facultad para el órgano de investigación de acceder a información confidencial contenida en bancos de datos, reservada a la esfera personal del individuo, sin que medie la autorización judicial previa, está estableciendo una interferencia indebida en el ejercicio del derecho fundamental a la intimidad, que resulta efectivamente transgresora del artículos 14 C.P., así como del 250.3 ib. que establece los presupuestos bajo los cuales el Estado, en legítimo ejercicio de su potestad investigativa, puede realizar intervenciones en los derechos fundamentales.

La información confidencial o los datos personales contenidos y procesados en bancos de datos, en la mayoría de los países del mundo están celosamente protegidos. Especialmente la Comunidad Europea a través de la Directiva 95/46/CE, del Parlamento y Consejo Europeo define los bancos de datos como *“todo conjunto estructurado de datos (en este caso, personales), centralizados o repartidos en diversos emplazamientos y accesibles con arreglo a criterios determinados, que tengan por objeto o efecto facilitar la utilización o el cotejo de datos relativos a los interesados”*.

La misma directiva define datos personales como *“toda información sobre una persona física identificada o identificable” (el interesado); considerando “identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social”*.

¹ Corte Constitucional, sentencia C-336 de 2007. M.P. Jaime Córdoba Triviño.

TRATAMIENTO DE DATOS PERSONALES EN EL PROCESO PENAL COLOMBIANO. TÉCNICA JUDICIAL.

La mencionada Directiva establece que “no se considerarán de carácter personal los datos reunidos en estadística de tal modo que los interesados dejan de ser razonablemente identificables”, como ocurre con los datos capturados por el DANE².

Así mismo, en el art. 8 ejusdem establece que “los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad” estos son los denominados datos sensibles.

En el ámbito europeo la Convención para la protección de los individuos con relación al procesamiento automático de datos personales, conocida como la Convención de Estrasburgo y suscrito por veintinueve estados europeos (el 21 de enero de 1981) ha constituido el antecedente más importante en la materia. Al compás de este movimiento los países fundamentalmente europeos sancionaron una serie de leyes desde la primera, del Land de Hesse de la ex-República Federal de Alemania (7-10-70), la ley federal alemana de 1977 (*Federal Data Protection Law*); la ley sueca sancionada el 11-5-1973; la ley francesa sobre Informática, ficheros y libertades (6-1-78), la ley federal de Austria sobre Protección de Datos Informáticos de índole personal (18-10-78); las leyes de Dinamarca, *Public Authorities Register Act* (1991) para el sector público y *Private Registers Act* (1987) para el sector privado; la legislación de Noruega (1978); Finlandia (ley 471/87) hasta las más recientes de Portugal (ley 10/91 del 9-4-91); Hungría (1992); Bélgica (8-12-92); España Ley Orgánica 5/92 de Regulación del Tratamiento de Datos (LORTAD) modificada parcialmente por la Ley de Protección de Datos Personales 15/1999, Italia (1996), Grecia (1997) y Gran Bretaña aprobó la *Data Protection Act* (1998).

En Latinoamérica existen dos países con leyes puntuales sobre Protección de Datos como son la Mexicana con la Ley federal de Transparencia y Acceso a la Información Pública Gubernamental y crea el Instituto Federal de Acceso a la Información Pública, es la que hace cumplir los lineamientos de protección de Datos Personales; y en Argentina la Ley 25326 de Octubre 4 de 2000, crea una entidad denominada Dirección Nacional de Protección de Datos Personales y la acción de protección de datos. En Chile la Ley 19.628, se refiere a la Protección de la Vida Privada, pero no es concretamente una ley de protección de datos, además no existe entidad que los proteja.

En Colombia el Dr. Nelson Remolina³ afirma en su blog, que cada vez son más visibles los esfuerzos regulatorios de varias entidades en el camino indicado. Dos ejemplos de ello son las resoluciones de la Comisión de Regulación de Telecomunicaciones y el decreto 1151 del 14 de

² En Colombia el DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA, es la entidad responsable de la planeación, levantamiento, procesamiento, análisis y difusión de las estadísticas oficiales de Colombia. Perteneciente a la Rama Ejecutiva del Estado Colombiano, con más de 50 años de experiencia, el DANE cumple con los más altos estándares de calidad (ISO 9001:2000). El DANE ofrece al país y al mundo más de 30 investigaciones de todos los sectores de la economía, industria, población, sector agropecuario y calidad de vida, entre otras. Información obtenida de la vista al site del DANE <http://www.dane.gov.co/> el 24 de Agosto de 2008, a las 6:37 pm.

³ Dr. Nelson Remolina. Director de Pregrado de la Facultad de Derecho de la Universidad de Los Andes-Bogotá Colombia. Visita realizada a su blog en la siguiente url <http://www.habeasdata.org.co/> el día 24 de agosto de 2008, a las 7:36 pm.

abril de 2008 en donde la “*protección de la información del individuo*” es uno de los principios aplicables a la estrategia de gobierno en línea. Que se suma a ello, el proyecto de ley estatutaria 221/07 Cámara acumulado con el 05/06 Senado que está a punto de convertirse en ley, pues está en trámite el control automático de la Corte Constitucional. Agrega que este será el marco de referencia para la adecuación ante la Comisión Europea. Se refiere también que se trata de un texto con importantes aciertos en la materia pero notablemente insuficiente frente a los estándares europeos de protección de datos personales pues considera que ésta contiene algunas falencias a saber:

1. Carencia de una autoridad de control general e independiente: El esquema del proyecto prevé que la Superintendencia financiera y la Superintendencia de Industria y Comercio harán las veces de autoridad de control únicamente respecto de la información comercial y financiera. Deja por fuera el control sobre datos respecto de la salud, sensibles, laborales, etc. No debe perderse de vista que el proyecto de ley fue concebido, ante todo, como una ley para las centrales de información financiera. Esta es la causa por la cual no contaremos con una verdadera ley estatutaria de protección de datos personales a tono con los estándares internacionales.

Resalta que los superintendentes carecen de independencia porque son funcionarios de libre nombramiento y remoción. No tienen un término fijo para el ejercicio de sus funciones y hacen parte del gobierno nacional que, al mismo tiempo, es uno de los principales administradores de datos personales, lo que implica que la protección de los datos se someterá a los vaivenes del gobierno de turno.

2. No incorporación de principios y derechos fundamentales en materia de protección de datos personales: Se omiten los siguientes: (1) Principio de transparencia, (2) Aspectos sobre decisiones individuales automatizadas y (3) derecho de oposición al tratamiento

3. Omisión de regulación de datos especiales: El proyecto es mudo respecto del tratamiento de la información sensible y de los datos personales de las niñas y los niños.

4. Inconsistencia abierta con las reglas del flujo internacional de datos personales. El literal f) del artículo 5 del proyecto es problemático pues concede al operador, y no a la autoridad de control, la facultad de establecer si un país diferente a Colombia garantiza un nivel adecuado de protección. En Europa esta situación la define la Comisión Europea cuando concede el nivel de adecuación a un país o las autoridades de control de cada país.

Termina diciendo que estos son algunos aspectos que se deben tener en cuenta en Colombia a la hora de modificar la futura ley estatutaria pues se quedó corta frente a los estándares internacionales. Tampoco está a la altura del nivel de protección de los datos personales que merecemos los colombianos. Paradójicamente contamos con un texto constitucional de lujo pero con una futura ley que deja mucho que desear en ciertos tópicos. En Colombia la protección de datos se realiza a través de una acción de tutela, no existe acción independiente o autónoma como si ocurre en otras naciones.

En España, la protección de datos personales goza de la más alta protección constitucional, pues en el art. 18 inciso 4: *La ley limitará el uso de la información para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de los derechos*, artículo incardinado en la Sección 1ª, Capítulo II del Título Primero, que según el art. 53. 1. vinculan a todos los poderes

públicos. Sólo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades, y además, cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos en el art. 14 y la Sección primera del Capítulo 2º ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumario y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional.

Ahondaremos más adelante con el tema de la protección de los datos personales, porque pasaremos a realizar algunos comentarios sobre los datos personales hallados en dispositivos telefónicos móviles como son: MMS, EMS, SMS, pero antes, se torna necesario que nos refiramos previamente a las comunicaciones inalámbricas a través de dispositivos móviles, llamados celulares.

1. TELEFONÍA CELULAR

La telefonía celular es un sistema de comunicación telefónica totalmente inalámbrica, en este caso los sonidos se convierten en señales electromagnéticas, que viajan a través del aire, siendo recibidas y transformadas nuevamente en mensaje a través de antenas repetidoras o vía satélite.

El área que cubre una antena es una célula. Los encargados de diseñar el prototipo final de la telefonía móvil, fueron los científicos del laboratorio Bell, quienes después de muchos intentos inspirados en los radioteléfonos, dieron inicio a la telefonía celular en 1983, extendiéndose a nivel mundial.

En Colombia, la telefonía móvil llegó en 1994, dando inicio a la libre competencia en el sector de las telecomunicaciones, rompiendo con una larga tradición de monopolio y proteccionismo por parte del estado. Actualmente son tres las compañías que distribuyen el servicio en la totalidad del territorio nacional

Los teléfonos celulares, por sofisticados que sean y luzcan, no dejan de ser radio transmisores personales. Para entender mejor cómo funcionan estos sofisticados aparatos puede ayudar compararlos con una radio de onda corta (OC) o con un walkie-talkie. Un radio OC es un aparato simple. Este permite que dos personas se comuniquen utilizando la misma frecuencia, así que sólo una persona puede hablar al tiempo.

Un teléfono celular es un dispositivo dual⁴, esto quiere decir que utiliza una frecuencia para hablar, y una segunda frecuencia aparte para escuchar. Una radio OC tiene 40 canales. Un teléfono celular puede utilizar 1664 canales. Estos teléfonos también operan con "células" (o "celdas") y pueden alternar la célula usada a medida que el teléfono es desplazado. Las células le dan a los teléfonos un rango mucho mayor a los dispositivos que lo comparamos. Un walkie-talkie puede transmitir hasta quizás una milla. Una radio OC, debido a que tiene un poder mucho más alto, puede transmitir hasta 5 millas. Alguien que utiliza un teléfono celular, puede manejar a través de

⁴ Telefonía Celular. Trabajo de investigación encontrado en el site <http://www.monografias.com/trabajos34/telefonía-celular/telefonía-celular.shtml> en visita realizada el 23 de Agosto de 2008 a las 10:11 pm

TRATAMIENTO DE DATOS PERSONALES EN EL PROCESO PENAL COLOMBIANO. TÉCNICA JUDICIAL.

U.S. Department of Justice
Criminal Division
*International Criminal
Investigation and Training
Program (ICITAP)*

toda la ciudad y mantener la conversación todo el tiempo. Las células son las que dan a los teléfonos celulares un gran rango.

La particularidad que distingue a la telefonía móvil celular reside en que una ciudad puede ser dividida en pequeñas "células" (o celdas), que permiten extender la frecuencia por todo el territorio de la comarca. Esto es lo que permite que millones de usuarios utilicen el servicio en un territorio amplio sin tener problemas.

He aquí como funciona. Se puede dividir un área (como una ciudad) en células. Cada célula es típicamente de un tamaño de unos 26Km². Las células se imaginan como unos hexágonos en un campo hexagonal grande.

Sin embargo, el tamaño de las células puede variar mucho dependiendo del lugar en que se encuentre. Las estaciones de base se separan entre 1 a 3 Km. en zonas urbanas, aunque pueden llegar a separarse por más de 35Km en zonas rurales.

En zonas muy densamente pobladas o áreas con muchos obstáculos (como ser edificios altos), las células pueden concentrarse en distancias cada vez menores. Algunas tecnologías, como los PCS (Personal Communication Services), requieren células muy cercanas unas de otras debido a su alta frecuencia y bajo poder en el que operan.

Cada celda en un sistema análogo utiliza un séptimo de los canales de voz disponibles. Eso es, una celda, más las seis celdas que la rodean en un arreglo hexagonal, cada una utilizando un séptimo de los canales disponibles para que cada celda tenga un grupo único de frecuencias y no haya colisiones entre células adyacentes.

Cada célula tiene una estación base que consta de una torre y un pequeño edificio en donde se tiene el equipo de radio. Cada célula utiliza un séptimo de los 416 canales duales de voz. Dejando entonces a cada célula aproximadamente los 59 canales disponibles nombrados anteriormente.

Si bien los números pueden variar dependiendo de la tecnología usada en el lugar, las cantidades sirven para mostrar cómo funciona esta tecnología; que en caso de tratarse de una generación más moderna, puede de todas formas extrapolarse directamente.

Los teléfonos celulares poseen unos transmisores de bajo poder dentro de ellos. Muchos teléfonos celulares tienen 2 fuerzas de señal: 0.6 Watts y 3 Watts (como comparación, la mayoría de los radios de onda corta transmiten a 5 Watts). La estación base también transmite a bajo poder. Los transmisores de bajo poder tienen 2 ventajas:

Las transmisiones de las estaciones base y de los teléfonos no alcanzan una distancia más allá de la célula. Es por esto que cada celda se puede utilizar las mismas frecuencias sin interferir unas con otras. Las transmisiones de la base central y de los teléfonos en la misma celda no salen de ésta. Por lo tanto, cada celda puede reutilizar las mismas 59 frecuencias a través de la ciudad.

La tecnología celular requiere un gran número de estaciones base para ciudades de cualquier tamaño. Una ciudad típica grande puede tener cientos de torres emisoras. Pero debido a que hay tanta gente utilizando teléfonos celulares, los costos se mantienen bajos para el usuario. Cada

portador en cada ciudad tiene una oficina central, esta oficina maneja todas las conexiones telefónicas y estaciones base de la región.

Cuando el usuario desea realizar una llamada, el teléfono celular envía un mensaje a la torre solicitando una conexión a un número de teléfono específico. Si la torre dispone de los suficientes recursos para permitir la comunicación, un dispositivo llamado "switch" conecta la señal del teléfono celular a un canal de la red de telefonía pública. La llamada en este momento toma un canal inalámbrico así como un canal en la red de telefonía pública que se mantendrán abiertos hasta que la llamada se concluya.

Digamos que usted tiene un celular, lo enciende, y alguien trata de llamarle. La oficina central recibe la llamada, y trata de encontrarlo. Desde los primeros sistemas la oficina central lo encontraba activando su teléfono (utilizando uno de los canales de control, ya que su teléfono se encuentra siempre escuchando) en cada célula de la región hasta que su teléfono respondiera. Entonces la estación base y el teléfono decidirán cuál de los 59 canales en su teléfono celular usará. Ahora estará conectado a la estación base y puede empezar a hablar y escuchar.

A medida que usted se mueva en la célula, la estación base notará que la fuerza de su señal disminuye. Entretanto, la estación base de la célula (receptora-transmisora), le vincula su equipo a la siguiente célula (área de influencia de la siguiente antena), hacia donde se está moviendo (que está escuchando la señal) y esta será capaz de notar que la señal se hace más fuerte.

Las dos estaciones base se coordinan a sí mismas a través de la oficina central y en algún punto su teléfono obtiene una señal que le indica que cambie de frecuencia. Este cambio hace que su teléfono mude su señal a otra célula.

En sistemas modernos los teléfonos esperan una señal de identificación del sistema (IDS) del canal de control cuando se encienden. El teléfono también transmite una propuesta de registro y la red mantiene unos datos acerca de su ubicación en una base de datos (de esta forma es que la oficina central sabe en que célula se encuentra si quiere timbrar su teléfono). A medida que se mueve entre células, el teléfono detecta los cambios en la señal, los registra y compara para con los de la nueva célula cuando cambia de canal. Si el teléfono no puede hallar canales para escuchar se sabe que está fuera de rango y muestra un mensaje de "sin servicio".

Éste es, en forma bastante simplificada, el funcionamiento de la telefonía celular; abarcando desde el aspecto teórico en la división de las zonas geográficas en células, hasta el intercambio de ondas electro magnéticas necesario para establecer una sencilla comunicación entre dos teléfonos celulares.

2. SERVICIO DE MENSAJERÍA

2.1. SMS. Short Messaging Service, servicio de envío de mensajes cortos, es su significado de sus siglas en ingles. Sistema que todo el mundo lo utiliza pero muchos no saben lo que significan. Aunque de momento se seguirán enviando este tipo de mensajes, sobre todo por parte de los usuarios más jóvenes, servicio que tiene al parecer sus días contados. Las empresas de telefonía que se han dedicado a invertir en los últimos tiempos en el desarrollo en la telefonía móvil celular, ha dirigido su atención a los MMS (Multimedia Messaging Service). En donde se seguirán enviando

los mensajes entre celulares, pero ya no se reducirán a un simple texto de 160 caracteres, sino que les podrá añadir imágenes, vídeos y sonido. Como puente para que esto llegue a buen puerto y además para empezar a crear una demanda entre los usuarios, algunas empresas se han lanzado a una tecnología intermedia llamada EMS (Enhanced Messaging Service). Como tecnología intermedia que se precie, está entre su antecesor y el resultado de su evolución, de este modo permite enviar sonidos, texto e imágenes pero éstas últimas sólo en blanco y negro.

2.2. MMS. Según algunos estudios mensualmente se calcula que se envían en todo el mundo 20.000 millones de mensajes y se estima que el 80 por ciento de éstos son personales, el resto comercial o publicitario. El éxito de los SMS se debe a que todos los móviles son compatibles independientemente de la marca y el modelo de cada terminal y por el bajo coste de los mensajes, y resulta además más barato que una llamada telefónica. Por otra parte, tanto las operadoras como empresas de contenidos y servicios se subieron al tren de los SMS y ofrecen a los usuarios infinidad de servicios, en algunos casos gratuitos.

Por otro lado, los llamados chats para móviles han beneficiado a todo el mundo, ya que los mensajes suelen tener un coste muy bajo, pero los usuarios no se limitan a enviar uno solo. Lo último que se ha lanzado para aumentar los ingresos de las empresas es la posibilidad de recibir logos o melodías, pero estas opciones no son válidas para todos los teléfonos. También permiten la votación en programas de televisión o radio a través del envío de un mensaje, con precios especiales, es decir, más caros, pero por otra parte más barato que la llamada a un número 901.

2.3. EMS. Enhanced Messaging Service (EMS) o Servicio de Mensajería Avanzada ya se puede utilizar en muchos terminales que ya se comercializan; teléfonos dirigidos principalmente a gente joven, ya que este público es el que utiliza más los servicios de chats y la tecnología EMS permite enviar mensajes más largos. Pero la gran ventaja de los nuevos mensajes de texto a través del móvil es que son compatibles con los ya famosos SMS, por lo que no te obligan a comprar otro terminal para poder recibir este tipo de mensajes.

EMS fue inventado con Ericsson y funciona sobre las redes GSM, pero más tarde se subieron a carro Siemens y Motorola. A muchos de nosotros nos extraña que Nokia no haya querido que sus usuarios formen parte de la comunidad de los EMS, pero la razón es bastante sencilla, por un lado la compañía cuenta con una tecnología para enviar mensajes con imágenes entre algunos terminales de la propia compañía, pero que no son compatibles con teléfonos de otras compañías, incluso se podían enviar por infrarrojos ahorrándonos la llamada telefónica o el mensaje, esto ocurría con el modelo 8210 por ejemplo. La otra razón, es que Nokia no está dispuesta a invertir dinero en una tecnología que será reemplazada por los MMS en un corto periodo de tiempo. Pese a esto, algunos estudios y responsables de ciertas compañías aseguran que EMS será la primera toma de contacto para MMS, es decir el puente hacia UMTS.

Pero como mensajería avanzada, como el propio nombre indica, se trata de la evolución de los SMS, ahora con más posibilidades. En primer lugar no se limitan a los 160 caracteres que todos conocemos, también se pueden enviar imágenes estáticas o en movimiento y melodías. Eso sí, para poder recibir esto último el teléfono móvil que lo recibe si tiene que ser compatible con EMS. Otras posibilidades que permite la mensajería avanzada es la posibilidad de tratar el texto, es decir, subrayar palabras o frases, ponerlas en negrita o tachadas, alinear el texto a la derecha, a la izquierda o simplemente escribirlo centrado, así como modificar el tamaño de las letras. Otras ventajas que podemos señalar es que por regla general la tecnología EMS se incorpora en

TRATAMIENTO DE DATOS PERSONALES EN EL PROCESO PENAL COLOMBIANO. TÉCNICA JUDICIAL.

teléfonos móviles que soportan GPRS, lo que facilitará bajar logos y melodías de Internet, pero además se pueden personalizar, a través de un software incluido en el propio teléfono, y reenviar posteriormente.

3. BÚSQUEDA SELECTIVA EN BASE DE DATOS.

Al iniciar este trabajo enunciábamos como la Corte Constitucional se ha pronunciado sobre el tema, en sentencia de constitucionalidad C-336/07, cuando en ejercicio de la acción pública consagrada en el artículo 241 de la Constitución Política de Colombia, se solicitó la declaratoria de inconstitucionalidad parcial de los artículos 14, 244 y 246 de la Ley 906 de 2004, la que se conoce en nuestro país como el Código de Procedimiento Penal.

Arguye el actor de entonces que el texto: **“cuando resulte necesaria la búsqueda selectiva en las bases de datos computarizadas, mecánicas o de cualquier otra índole que no sean de libre acceso o”** contenido en el artículo 14 y el: **“deberá mediar autorización previa del fiscal que dirija la investigación y”** del inciso segundo del artículo 244 ibídem. Éstas son manifiestamente contrarias al artículo 250 numeral 2º de la Carta y a la jurisprudencia constitucional que lo desarrolla, porque autorizan la búsqueda selectiva en bases de datos confidenciales con autorización previa del fiscal que dirija la investigación, sin obtener a respectiva autorización del juez que ejerce funciones de control de garantías, a pesar de que dicha medida investigativa implica afectación de derecho fundamental no está consagrada en los casos excepcionales como son los registro, allanamientos, incautaciones e interceptación de comunicaciones, en los que la Fiscalía puede proceder de esa manera, sin control previo del Juez, conforme lo señala el artículo 250 numeral 21 de la Constitución.

Finalmente esgrime que la expresión **“diferentes a las previstas en el capítulo anterior”** del artículo 246, considera que ésta agrega un condicionamiento no previsto en la Constitución para exigir orden judicial previa. Señala que el aparte demandado es inconstitucional por unidad normativa, ya que remite a un listado de excepciones que excede los cuatro eventos en que constitucionalmente la Fiscalía puede afectar derechos fundamentales por iniciativa propia y sin control previo del juez de garantías como son: allanamientos, registros, incautaciones, interceptaciones de comunicaciones.

La Corte Constitucional al analizar las circunstancias expuestas, afirma que el carácter de previo del control judicial, como regla, deriva del reforzamiento que en el sistema de investigación penal de tendencia acusatoria se imprimió al principio de reserva judicial de las intervenciones que afectan derechos fundamentales, pues las decisiones que los restringen son tomadas por los jueces o tribunales⁵. La afectación de derechos fundamentales en casos de requerirse medidas adicionales, obliga al Fiscal a solicitar de manera expresa y específica la autorización judicial previa.

El empleo del término afectación supone, según su grado, una limitación o restricción al ejercicio o goce de un derecho fundamental, como lo son los datos personales consagrados o protegidos por nuestra Constitución. Esto se articula a un sistema de información más complejo denominado banco de datos o central de información, con miras de racionalización y control del poder informático. Dijo la Corte un banco de datos no es otra cosa que un conjunto de informaciones que

⁵ Corte Constitucional, sentencia C-1092 de 2003. MP. Álvaro Tafur Galvis.

se refieren a un sector particular del conocimiento, las cuales pueden articularse en varias bases de datos y ser distribuidos a los usuarios de una entidad que se ocupa de constante actualización y ampliación.

La búsqueda selectiva de información en base de datos que no sean de libre acceso es aquella referida a un objeto o sujeto específico predeterminado o preestablecido, que reposa en bases de datos sometidas a régimen de divulgación restringido, ya sea porque se trate de materias que el Estado debe preservar para la protección del interés general y la seguridad nacional, o por razones de similar naturaleza. En cambio, la búsqueda selectiva en bases de datos que contengan información confidencial referida al indiciado o imputado, hace referencia a las búsquedas focalizadas sobre un sujeto en particular, en este caso a indiciado o imputado. La confidencialidad de la información dimana del carácter personal de los datos, cuya difusión constituye una invasión a la intimidad personal o familiar de su titular. La confidencialidad, es uno de los principios que regla al actividad del tratamiento de datos personales, en virtud del cual, las personas que intervengan en la recolección, almacenamiento, uso, divulgación y control de estos datos están obligadas, en todo tiempo, a garantizar la reserva de la misma, incluso después de finalizar su relaciones con el responsable del tratamiento.

Los datos personales capturados en una base de datos, pueden ser buscados y colectados en formas diferentes. Este tipo de búsqueda admite así mismo la posibilidad de elaborar reportes que cruzan variables a través de filtros para visualizar la información desde un determinado punto de referencia, según los criterios de quien quiere realizar la búsqueda. Por ello he diseñado una especie de formulario para personal de la Policía Judicial (CTI, DIJIN, SIJIN, DAS) y los mismos Delegados Fiscales, que consiste en realizar peticiones al Juez de Control de Garantías sobre aspectos que cubran todos los rincones de la investigación, tenemos entonces como atrás lo reseñábamos sobre los dispositivos telefónicos móviles, los que poseen entre otras herramientas, el poder conservar datos y muchos de ellos personales.

En una solicitud de autorización de control de garantías (pre o pos) hemos de enumerar qué ficheros han de abrirse, recolectarse, interpretarse, relacionarse e imprimirse si fuere necesario; datos capturados en el dispositivo telefónico, si el fabricante le ha permitido esa configuración al equipo o sino en la tarjeta sim, conocida también como SIMCARD y ellos son:

3.1. Ficheros Geográficos:

Arriba explicábamos como las comunicaciones inalámbricas móviles (telefonía celular) se logran a través de muchas antenas o celdas, sembradas en diferentes partes del territorio de influencia del operador del servicio de telefonía móvil celular, que permiten la interconexión de voz entre múltiples usuarios. Cada celda o antena tiene su identificación autónoma, que informa las características de la antena, lugar en donde se encuentra apostada, capacidad de alcance y otros datos que son caprichosos para su identificación dados por el operador del servicio.

Con esta identificación podemos establecer desde qué celda o antena (lugar del país o ciudad, dirección aproximada) se hacen o se hicieron las mayoría de las llamadas implicadas en el reato por el indiciado o imputado. Igualmente podemos establecer en que partes del territorio nacional se desplazó éste, cuantas llamadas realizó desde aquel lugar o punto geográfico, a qué horas y a qué destinos (usuarios propios del operador o diferentes), como también cuántas y desde qué números y en dónde se encontraban aquellos para cuando recibió los telefonemas. Estos datos son o

TRATAMIENTO DE DATOS PERSONALES EN EL PROCESO PENAL COLOMBIANO. TÉCNICA JUDICIAL.

pueden ser importantes, porque los delincuentes pueden usar tarjetas hurtadas o compradas en el mercado negro de estos dispositivos que se ha generados desde cuando se implementó este servicio en el país, resultando inane buscar en ficheros biográficos para establecer la identidad del titular del usuario del servicio, finalmente establecemos que quien aparece como titular del equipo es una persona tal vez muere, pues se le perdió o se la hurtaron en vida (pensemos en un adulto mayor) y no tiene nada que ver con el asunto criminal.

3.2. Ficheros Biográficos

Son los datos personales registrados del abonado o usuario del servicio, para cuando se suscribió al servicio del operador de telefonía. Resulta eficaz esta búsqueda, siempre y cuando, contemos con la suerte que el titular del equipo y servicio es el mismo delincuente, lo que no siempre es así. No obstante podemos saber a quien le perteneció el equipo, puede ocurrir muchas veces que los delincuentes están usando el dispositivo de la propia víctima (v.g. Un secuestrado); podemos también realizar varios procesos de descartes o filtrado, como se establece que se trata de un equipo prepago, que el usuario se adquirió la simcard con un equipo no suministrado por el operador etc. Bueno, logrado identificar el titular del dispositivo telefónico podemos aproximarnos o no a los titulares de la acción penal.

En este fichero se puede establecer también los datos personales de los titulares de los teléfonos fijos y móviles a quienes se les hicieron llamadas desde este dispositivo o número telefónica ora de los que le hicieron llamadas al titular del dispositivo o simcard sub judice.

3.3. Ficheros de Tráfico

En éste se captura el número de llamadas telefónicas que se realizaron con el dispositivo telefónico y/o con el número de suscriptor. Con ella establecemos también, los números de teléfonos móviles o fijos a donde se hicieron llamadas telefónicas, fecha de estas, duración de las mismas y si existe orden de interceptación, lograremos contenidos de las comunicaciones cruzadas por el indiciado o imputado con terceros u otros interlocutores posiblemente vinculados a la investigación.

Se hace necesario resaltar que no es indispensable, más bien pensaría que se torna violatorio de derechos fundamentales, incluir llamadas como a NÚMEROS CALIENTES, ni el número como tampoco su contenido, que en nada va a servir para la investigación a no ser que se trate de conductas que violen bienes jurídicamente tutelables como la libertad, integridad y formación sexuales, entre otros; esto es, una conversación de un usuario (así esté sub judice) de una de estas líneas de preferencias sexuales, nada tiene que ver con un reato contra la vida o el patrimonio económico v.g.

Igualmente se deben desestimar las imágenes de alto contenido sexual o pornográfica remitidas a través de MMS (a no ser que sean pedófilas u otro género), éstas no deben ser parte, si son fijas, en un álbum para relacionar el acontecer fáctico de la víctima o victimario, seguramente se le ordenará al Delegado Fiscal su exclusión y tal vez una amonestación por violación de los datos (sensibles) personales del implicado. Igual suerte deben correr las imágenes móviles conservadas y creadas en ficheros autónomos (teléfonos con videograbadoras) o recibidas o remitidas desde estos dispositivos, si no son de de la trascendencia procesal debida y constitucional. Suerte similar

corren con los datos personales de tipo familiar que no tengan nada que ver con la situación fáctica procesal investigada por la Fiscalía General de la Nación.

Se debe solicitar también qué número de llamadas se realizaron con alguna frecuencia a algún número determinado (v.g. a un copartípe) y desde cuál recibió más, estableciéndose el vínculo entre éste o estos abonados, como cercanía geográfica (vecinos, compañeros de trabajo) familiares, comerciales, patrimoniales, laborales, políticos, judiciales (v.g. empresa criminal) horario y preferencia de éste, a las tres de la tarde o dos de la madrugada.

En este estudio hay que ser muy cuidadosos, porque se han perdido días de trabajo, al realizarse investigaciones sobre días o períodos de tiempo no solicitados, ni autorizados. Si hablamos v.g. del seis de diciembre de dos mil siete al veintitrés de marzo de dos mil ocho, no puede ser días anteriores ni uno más superando la fecha límite. Se irán a excluir y tal vez aquellos, los no considerados (ilegales), sean los más importantes de la investigación.

3.4. Ficheros de Mensajería de texto.

Se deben solicitar al operador, si no se tiene el dispositivo telefónico móvil, la recuperación, revisión, reconstrucción (si existen fragmentos) de lo existente en los ficheros conservados por el operador en su base. Se solicitarán los mensajes, como arriba los relaciono, los SMS (Short Messaging Services) los MMS (Multimedia Messaging Services) y los EMS (Enhanced Messaging Service) y los demás sistemas a medida que vayan saliendo al mercado en razón a la investigación tecnológica, en donde a través de mensajes de texto, video y voz, se cruzan diferente información clave para la investigación penal, entre los individuos vinculados por la Fiscalía.

Los resultados de la petición deberán contener los números de teléfonos que intervinieron en el mensaje, fecha, titular de los números o dispositivos si se lograra o tuviera esa información el operador, residencia de los mismos, identificación ciudadana de los intervinientes, contenido de los mensajes, si existe mensajes MMS con imágenes fijas o móviles, establecer si no contiene mensajes ocultos. Ciudad o ciudades, municipios y/o país desde donde se cruzaron la información capturada.

3.5. Ficheros de Mensajería de Voz

Son los mensajes que dejan los interlocutores en el buzón del usuario del sistema a viva voz. Existen operadores que los mensajes de voz los convierten en mensajes de texto o MMS y a contrario sensu los mensajes de texto los convierten en mensajes de voz. No obstante el historial de dicha herramienta reposa en los ficheros de los operadores, en Europa se ha expedido una directiva en una se ha ordenado seis meses, en Argentina se ha intentado lo mismo, pero la idea ha sido desechada en razón de lo costosa que resulta conservar la información durante ese período.

CONCLUSIONES

La Corte Constitucional Colombiana⁶ se ha referido sobre la búsqueda selectiva de información personal en bases de datos, considerando que se constituye un medio específico para la obtención de evidencia física con fines probatorios que conserva su propia autonomía, frente esos otros medios de acopio informativo relacionados en el numeral 2º del artículo 250 de la Constitución como son los registros, los allanamientos, las incautaciones y la interceptaciones de comunicaciones. Acertadamente y poniéndose a tono con el uso de las nuevas tecnologías ha concluido que ni técnica ni conceptualmente es posible, incluir la búsqueda selectiva de información en bases de datos en la categoría de los registros como instrumento de pesquisa, a los que se refiere el artículo 250.2 de nuestra Constitución Nacional, por ello se requiere la anuencia del Juez de Control de Garantías en los procesos penales, pues éstos no pueden confundirse con aquellos sistemas de información creados por el usuario que no ejercen esa actividad de acopio de información de manera profesional o institucional; la intervención que se realiza sobre los datos personales pueden comprometer el derecho al hábeas data y el derecho de la intimidad, de ahí el porque se requiere el juicioso estudio del Juez Constitucional para que analice la viabilidad de la prueba solicitada ora la legalización de los resultados.

Sabemos que la búsqueda selectiva en bases de datos, aunque se trata de una herramienta de valiosas posibilidades técnicas, cuando se usa en el tratamiento de datos personales, debe estar sometida a controles en virtud del principio de *individualidad* que rigen la administración de las bases de datos según el cual las administradoras deben mantener separadamente las bases de datos que se encuentren bajo su administración, de tal manera que queda prohibida la conducta dirigida a facilitar cruce de datos a partir de la acumulación de informaciones provenientes de diferentes bases de datos. No debemos descartar el riesgo que genera el uso de las bases de datos, nuestro Tribunal constitucional en su sentencia T-414 de 1992, así lo advirtió: *"Es preciso, de otra parte, recordar que a partir de la década del cincuenta máquinas tales como los computadores han hecho posible no sólo crear e interconectar enormes "bancos de datos" que pueden suministrar inmediatamente una vasta cantidad de información personal a grandes distancias y en forma más comprensiva, sino también establecer correlaciones entre datos que aisladamente son las más de las veces inofensivos pero que reunidos pueden descubrir aspectos cuya revelación atenta contra la libertad e intimidad del ciudadano."*

Alexander Díaz García. Abogado de la Universidad Católica de Colombia; Especialista en: Ciencias Penales y Criminológicas de la Universidad Externado de Colombia; Ciencias Constitucionales y Administrativas de la Universidad Católica de Colombia y Nuevas Tecnologías y Protección de Datos de la Escuela de Gobierno y Políticas Públicas de Madrid adscrita al Instituto Nacional de Administración Pública de España. Autor del libro en soporte papel **DERECHO INFORMÁTICO ELEMENTOS DE LA INFORMÁTICA JURÍDICA**, Editorial Leyer y de los siguientes trabajos de investigación: **EFFECTOS JURÍDICOS DE LOS DOCUMENTOS ELECTRÓNICOS EN COLOMBIA. Estudio de la Ley 527 de 1999. DESVINCULACIÓN DEL SERVIDOR PÚBLICO POR USO IMPROPIO DEL EMAIL OFICIAL. LA ÉTICA EN EL DERECHO INFORMÁTICO. LA PROTECCIÓN DEL DATO EN EL CONTEXTO JUDICIAL COLOMBIANO. ACCESO RETOS Y REALIDADES DE LA ADMINISTRACIÓN DE JUSTICIA EN COLOMBIA CON EL USO DE LOS MEDIOS ELECTRÓNICOS. ACCESO A LA ADMINISTRACIÓN DE JUSTICIA A TRAVÉS DE LAS NUEVAS TECNOLOGÍAS. DESNATURALIZACIÓN DEL DOCUMENTO ELECTRÓNICO JUDICIAL EN LA**

⁶ Corte Constitucional, T-729 de 2002. Magistrado Ponente: **Dr. EDUARDO MONTEALEGRE LYNETT** Bogotá D.C., cinco (5) de septiembre de dos mil dos (2002).

TRATAMIENTO DE DATOS PERSONALES EN EL PROCESO PENAL COLOMBIANO. TÉCNICA JUDICIAL.

U.S. Department of Justice
Criminal Division
*International Criminal
Investigation and Training
Program (ICITAP)*

APELACIÓN DE LA SENTENCIA EN EL SISTEMA PENAL ACUSATORIO (EL JUICIO ORAL) COLOMBIANO. MANEJO DE DATOS SENSIBLES EN FICHERO CLÍNICOS. Autor de la primer proceso judicial electrónico tramitado en la Internet, protegiendo los Derechos Fundamentales de Hábeas Data y la Intimidad Virtual, a través de una acción de tutela virtual, violado por abuso de spam. Facilitador de la Escuela Judicial Rodrigo Lara Bonilla, en los módulos de **INTERPRETACIÓN JUDICIAL, JUECES DE PAZ, CONCILIACIÓN EN EQUIDAD PARA JUECES FORMALES Y TRANSVERSALIZACIÓN DE GÉNERO.** Ex-Catedrático de la Escuela de Administración Pública en el Módulo de Contratación Electrónica Estatal y de la Universidad Cooperativa de Ibagué con la materia Informática Jurídica y Asesor Académico de la Universidad de Ibagué Coruniversitaria. Actualmente Asesor Académico de la Dirección de Postgrados de la Universidad Santiago de Cali con los proyectos **JUZGADO VIRTUAL; ESPECIALIZACIÓN, MAESTRÍA Y DOCTORADO EN NUEVAS TECNOLOGÍAS Y PROTECCIÓN DE DATOS.** Y el proyecto de ley **DELITOS ELECTRÓNICOS.** Conferencista del Programa Internacional de Asistencia y entrenamiento en la Investigación Criminal ICITAP del Departamento de Justicia de los Estados Unidos, con el tema delitos electrónicos. Miembro de la Mesa de Trabajo de Seguimiento Legislativo de los Delitos Cibernéticos de la Dirección de Políticas Multilaterales del Ministerio de Relaciones Exteriores de Colombia. Es el titular en la actualidad del Juzgado Segundo Promiscuo Municipal de Rovira Tolima Colombia.