La evidencia digital eximiente de violación a la protección del dato personal a partir de la autorregulación*

Defense digital evidence of violation to the protection of personal data from the self

Recibido: Agosto 21 de 2014 - Evaluado: Octubre 31 de 2014 - Aceptado: Noviembre 24 de 2014

Ana María Mesa Elneser**

Para citar este artículo / To cite this Article
Mesa Elneser, A. M. (Enero-Junio de 2015). La evidencia digital eximiente de violación a la protección del dato personal a partir de la autorregulación.
Revista Academia & Derecho, 6(10), (119-156).

Resumen

La Protección al Dato Personal en Colombia es un Derecho Constitucional Fundamental regulado a partir de la expedición de la Ley 1581 de 2012, regulada ésta con los Decretos Reglamentarios 1377 de 2013 y 886 de

* Artículo inédito. Artículo de investigación e innovación. Producto de una investigación en el Doctorado en Derecho Procesal Contemporáneo en el marco del proyecto "La evidencia digital como medio cognitivo en Colombia en relación a la producción de la prueba", adscrito al Grupo de Investigación Ratio Juris de la Universidad Autónoma Latinoamericana UNAULA.

** Doctoranda en Derecho Procesal Contemporáneo. Abogada y Magíster en Derecho Procesal por la Universidad de Medellín, Especializanda en Derecho Informático y Nuevas Tecnologías por la Universidad de la Patagonia en Argentina. Docente de la Universidad Autónoma Latinoamericana UNAULA.
Correo electrónico: ana.mesael@unaula.edu.co.

2014, y el proyecto de circular publicado en febrero de 2014 para definir los lineamientos frente al registro de la base de datos nacional - RBD, fuente normativa determinante para establecer los límites de la disponibilidad de la información y los datos en relación con la restricción de uso y circulación de los mismos, basada siempre en los derechos del ciudadano frente a las empresas y entidades de gobierno, como son entre otros, la protección del dato, la intimidad y la privacidad. Aunado a ello la gestión del dato personal y la información traen consigo responsabilidades por parte de quien posee su guarda temporal o permanente, exigiéndosele la adopción de políticas, procesos y procedimientos integradas a la estructura de la organización principalmente en el ámbito de la seguridad de la información con miras a la mayor protección de la información, la seguridad informática en la búsqueda de una mejor infraestructura tecnológica operativa y de respuesta en atención a incidentes, y la evidencia digital como mecanismo técnico científico (Cano, 2010) para extraer los rastros del incidente pudiendo identificar si se está frente a la comisión de un delito o no. Es por ello que a partir de la exigibilidad en la protección del dato personal se encaran escenarios jurídicos que constituyen un eximente de responsabilidad toda vez que operar como justificantes para su manipulación, aun no existiendo autorización previa del titular o norma decretada por el Estado Colombiano.

Palabras clave: Protección al dato personal, evidencia digital, forense digital, intimidad y privacidad.

Abstract

Personal Data Protection in Colombia is a fundamental constitutional right regulated from the enactment of Law 1581 of 2012, it regulated the Regulatory Decrees 1377 of 2013 and 886 of 2014, and the draft circular published in February 2014 to define the guidelines against the registration of the national database - RBD, always based on citizens' rights against companies and government entities, such as among others, the protection of data, intimacy and privacy. Added to this, personal data management and information bring responsibilities by who has temporary or permanent guardian, exacted the adoption of policies, processes and integrated into the structure of the organization mainly in the field of security procedures information for the fuller protection of information, computer security in the search for improved operational and technological infrastructure responsive

attention to incidents, and digital evidence as technical mechanism scientist (Cano, 2010) to remove traces of the incident may identify whether it is in front of the commission of a crime or not. That is why from the enforcement in the protection of personal data legal scenarios that constitute a defense to liability since they operate as evidence for manipulation, even in the absence of prior authorization holder or regulation enacted by the Colombian State is facing.

Key words: Personal data, digital evidence, digital forensics, intimacy and privacy.

Introducción

El presente artículo tiene como finalidad llevar al lector a una reflexión frente a la ED[1] como eximente de responsabilidad frente a la protección del dato personal cuando su existencia depende de una norma imperativa del Estado o cuando depende de una norma autoreguladora, teniendo en cuenta que no es producto de una investigación científica, por el contrario son temáticas emergentes dadas en la investigación Doctoral que permiten plantearse escenarios temáticos correlacionados con la Evidencia Digital, en el *artículo el análisis* se presentan aproximaciones al origen del dato personal desde la época Nazi con una articulación contemporánea que permite vincular la UE[2] y la OCDE[3] dentro del discurso, reseñando responsabilidad que tiene toda persona sobre tratamiento del dato personal previamente autorizado por su titular mientras sea poseedor de éste.

Posteriormente se hace una breve reseña teórica y legal de la Evidencia Digital, en relación a su naturaleza jurídica, su producción y responsable de esta. Finalmente encontrará una triangulación temática que permite identificar lo justificante de una investigación de un delito frente al derecho de acceso, tratamiento y circulación del dato personal en manos de un Responsable o Encargante responsable de su protección, siendo este análisis importante en la escena normativa puesto que tanto la Protección del Dato Personal es un derecho como constitucional como lo es el Debido Proceso con el que se

1 ED es a partir de ahora equivalente a evidencia digital o digital evidence.
2 Unión Europea.
3 Organización para la Cooperación y Desarrollo Económico.

garantiza al ciudadano el acceso a la prueba, arts. 15 y 29 respectivamente de la Constitución política, evitándose excesos del poder autoregulatorio o del Estado, al delimitar los escenarios de permisibilidad o de prohibición para el tratamiento y circulación de la información y datos.

Problema de investigación[4]

Los delincuentes informáticos o Ciberdelincuentes son operadores del delito de una sociedad digital como medio de vida para la sociedad, un estilo cultural de sectores sociales empresariales, comerciales, educativos, delincuenciales, entre muchos más; estas personas carecen de nombre, rostros, pero se encuentran en relación a sus víctimas a un clic de distancia, operando en línea o por medio de herramientas tecnológicas de operación asincrónica; independiente del medio de comunicación, estas son principalmente imperceptibles, por ello los protocolos ISO de normalización de seguridad como son las 27000, 27001 y 27002, se enfocan a que las organizaciones que lo adopten establezcan protocolo de respuesta ante incidentes informáticos, evitando contaminar los rastros que deja el delincuente en la escena del delito, sea en un espacio físico o digital.

La investigación de conductas delincuenciales desplegadas en entornos digitales, se dan por adopción de protocolos forenses digitales, aspecto temático de gran importancia para este planteamiento del problema, situación de problema entre el juez y el científico investigador. Tal como lo señala Michele Taruffo en su libro la Prueba de los Hechos "el fenómeno cada vez más relevante y frecuente del uso de «prueba científica» demuestra que no sólo no hay impermeabilidad alguna entre la determinación judicial de los hechos y el uso de metodologías científicas, sino que cada vez es más habitual que los hechos sean determinados científicamente en el proceso. Permanece así inalterable el carácter de especificidad «cientificidad» de la prueba, derivado del hecho de que esta supone el uso de métodos y conocimiento que trascienden el saber del hombre medio, pero esto no impide que corresponda en todo caso al juez servirse de esas pruebas particulares en la determinación de los hechos. (Taruffo, 2011).

[4] Texto extraído de la tesina doctoral de la autora, aun sin divulgar. Universidad de Medellín. Doctorado en Derecho Procesal Contemporáneo.

Ello exige un examen pormenorizado del derecho a la intimidad y la privacidad del sujeto a nivel internacional desde la declaraciòn de los derechos humanos, donde se consagran como derechos fundamentales e inquebrantables, a su vez al realizar una interpretación analógica frente a la convención de cibercrimen de Budapest dada UE 2001, se obtiene como resultado la necesidad de replantear la regla de valoración a los derechos de intimidad y privacidad respecto de delitos informáticos o delitos tradicionales que involucren software y hardware, teniendo en cuenta que los rastros del delito solo quedan almacenados en archivos o ficheros, y en dispositivos o hardware generalmente de propiedad privada, los cuales son solo manipulables si existe acceso a ellos, para la obtención de esos rastros y construir la evidencia de los hechos, o la futura prueba procesal, sin ese acceso por ausencia de variaciòn en la ponderación de derechos fundamentales que hace el juez frente a la prueba, se genera como resultado una extrema protecciòn del investigado, y se legaliza una fuente generadora de impunidad a aprovechada por los cibercriminales, porque la falta de evidencia digital fundamente los hechos alegados en juicio, deja sin evidencia los argumentos de la imputaciòn, en consecuencia, sin prueba para condenar un hecho delictivo.

Siendo relevante, por medio del presente artículo, preguntarse:

¿Cómo debe limitarse la exigibilidad de Protección del Dato Personal al momento de la recolección y extracción de la Evidencia Digital necesaria como fuente o medio de prueba ante incidentes informáticos que vincula información y datos?

Metodología de la investigación

Para la producción del texto principal de la tesina doctoral, se ha ejecutado una metodología de revisión documental frente a las variables temáticas de Evidencia Digital, Intimidad, Privacidad y Protección del Dato Personal, como instrumentos de control que se interrelacionan en el proceso penal al momento de producción de la prueba con intervención de protocolos forenses digitales y perito informático.

El esquema planteado para llegar a la parte concluyente en razón de la problemática, necesariamente se enmarca en un análisis del derecho constitucional denominado Protección del Dato Personal, para equipararlo con el tipo de prueba denominado Evidencia Digital en su nivel de producción más

primario, momento en el cual, el operador judicial, convalida su legitimidad y validez, para categorizar la extracción como prueba digital.

Esquema de resolución

Para el abordaje del tema se ha estructurado el escrito en los siguientes temas: I. El dato personal y su protección; a. *Perspectiva internacional*, 1. Referentes históricos, 1.1. Alemania Nazi, 1.2. UE, 1.3. OCDE, 1.4. Aproximación al caso Norteamericano; b. *Perspectiva colombiana*, 1. Alcance de la protección ((DDI), 2014), 2. Caracterización del dato personal protegido, 3. Principio de responsabilidad demostrada. II. Mirada a la privacidad, intimidad y dato personal en relación. III. Evidencia digital, 1. Breve Mirada Internacional, 2. Breve Mirada Nacional, 3. Evidencia digital en relación con intimidad, privacidad y datos personales en *log*. IV. Conclusiones.

I. El dato personal y su protección

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.

a. Perspectiva Internacional

1. Referentes Históricos

Los orígenes de la Privacidad, la Intimidad y el Dato Personal, se dan con finalidades paralelas pero con un mismo núcleo, que confluye en la persona física y su esfera de protección a cargo del Estado y de las Organizaciones en general, además de las otras personas físicas con las que se posee relación directa o indirecta que poseen sus datos personales agrupadas o compiladas en bases de datos.

La privacidad es un derecho moral, inalienable y que existe para los seres humanos en general, mismo principio de la construcción del derecho a la privacidad, siempre con distinta exigibilidad de protección por parte del tercero

a partir del sujeto que lo ejerce, hecho que refleja más conexión axiológica de la privacidad con la intimidad, que con el dato personal por encontrarse más ligada en razón a cuestiones subjetivas del ser, de la persona en sí misma, del ejercicio de los derechos personalísimos.

En la misma lógica se puede afirmar que la protección de datos personales es un derecho que surge en función de determinados acontecimientos históricos que ocurrieron, que mostraron a la sociedad la posibilidad de recolección y acumulación de datos personales por parte de los Estados, permitiendo dar lugar a un abuso de poder y a la utilización indebida o ilegal en razón al uso con fines totalmente distintos para los cuales se pretendían en el momento de su recolección.

El surgimiento de la categoría de base de datos y banco de datos en respuesta a información en masa o multiplicidad de datos que solo pueden ser entendidos y procesados de forma organizada si se establece una compilación parametrizada. Además, el uso de computadoras y medios digitales, o cualquier otra herramienta no tan convencional pero pensada para su automatización lógica que permita su tratamiento y la obtención de la información requerida, como sería entendido un sistema de tratamiento de información.

No siendo menos importante, la operatividad de los Estados, desde su ejercicio político y económico, y el plano personal de sus ciudadanos fundado en la información y datos que merecen una normativación además de unificación de criterios en protección de datos personales, que deriven en armonización legislativa para beneficio de los ciudadanos a nivel mundial.

1.1. Alemania Nazi

Si nos remontamos a la época de la Alemania Nazi[5] cuando llega Hitler al poder empieza a realizar un proceso de búsqueda en determinadas herramientas que le permitieran poder identificar todas aquellas razas que él consideraba en contra de la concepción de la raza perfecta o "Raza Aria" entre los cuales, sin limitarse a ellos, estaban: los Judíos, de los Gitanos, Delincuentes, Homosexuales, Religiosos y de los Discapacitados.

5 Época entre 1933 y 1945.

Así es cómo surge la relación con IBM, de acuerdo a lo descrito por el autor sobre los fines de la época (Black, 2001):

> "Sólo después de haber identificado a los judíos – una tarea monumental y compleja que Hitler quería terminada de inmediato-, se podía lograr una eficiente confiscación de bienes, reclusión de ghettos, deportación, explotación laboral y, en última instancia, aniquilación. Era un trabajo de cruce de base de datos y un desafío de organización colosal que exigía una computadora. Por su puesto, en los años 30, las computadoras no existían".

Una de las herramientas que utilizo para compilar esta información respecto de toda la gente existente en el territorio alemán en muy poco tiempo, además que fuera un diseño absolutamente planificado y que permitiera hacer un estudio de cómo estaba compuesta la población Alemana fue el Censo Nacional (Black, 2001), contemplando preguntas de tipo de carácter violatorio de derechos fundamentales o personalísimos, y que tendrían directa confrontación con la mayoría de las leyes vigentes en materia de protección de datos personales. La materia de la cual se ocupaban estos interrogantes eran sobre datos como: la religión, los antecedentes étnicos, el origen étnico de la familia o núcleo familiar, la composición del árbol genealógico hasta el nivel de los abuelos, obteniendo de cada persona Censada el dato de padre y abuelo.

> La tecnología de las tarjetas perforadas se remonta a 1884. Herman Hollerith. Con la ayuda de estos sistemas adaptados a la medida de sus necesidades, Hitler pudo automatizar la persecución de los judíos. Los historiadores han manifestado siempre su sorpresa ante la velocidad y la precisión con que los nazis fueron capaces de identificar y localizar a los judíos europeos. El hecho es que se usó la tecnología de IBM para organizar desde la identificación de los judíos a través de censos, registros y programas de rastreo de antepasados, hasta el manejo de los ferrocarriles y la organización del trabajo de esclavos en los campos de concentración. (Black, 2001).

Tecnología para la recolección de datos personales más sofisticada del mundo, y sin necesidad de una herramienta computacional. Permitió que pudieran recolectar datos que establecieran un perfil tan detallado con base a aspectos de la edad, educación, domicilio, religión y genealogía, entre otros, de carácter relevante para perfilar lo que sería la Raza Aria y el objetivo militar de exterminio. Toda esta información fue recolectada, procesada y analizada, permitiendo al Tercer Reich hacer el exterminio masivo, con una

fuente directa, además evidencia al mundo la necesidad de legislar en materia de datos personales y la protección que éste debe tener ante la recolección, tratamiento y circulación del mismo.

1.2. Unión Europea UE

El convenio número 108 del 28 enero 1981 abre la normativa regulatoria en favor de las personas con respecto al tratamiento automatizado de datos personales, con el fin de garantizarle a la persona física su protección sin importar el territorio, nacionalidad o residencia, en relación con los derechos y las libertades, específicamente de sus datos personales. Posteriormente se emite la Directiva 95/46/CE dada a instancias del parlamento Europeo y del Consejo el 24 octubre 1995, regulando de forma directa para las personas físicas el tratamiento de datos personales y la libre circulación de éstos[6], siendo obligante para los estados miembros de la Unión la protección del dato personal a partir del ejercicio de las libertades y los derechos fundamentales de las personas físicas. Finalmente en el año 2000 la Unión Europea incluye en la Carta de Derecho Fundamentales el art. 8 que expresa "*1. toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan, 2. Estos datos se trataran de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la Ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación, y 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".*

Es a instancias de la Unión Europea donde más se ha reflexionado entorno a la protección del dato personales desde una perspectiva de utilización del dato de forma leal, adecuada, pertinente y no excesiva, siempre pensándose en el ciudadano y su derecho fundamental a que el dato sea protegido y amparado por quien es el guardador de éste.

1.3. OCDE[7]

El 14 diciembre de 1960 Canadá y EE.UU. se unieron a los miembros de la OPEP en la firma de un nuevo convenio internacional que daría vida a la

6 Ley de Protección de Datos L281 de 23/11/1995

7 Organismo internacional para la cooperación en el desarrollo económico.

Organización para la Cooperación y el Desarrollo Económico, que se oficializa con la entrada en vigor del acuerdo el 30 septiembre 1961. (OCDE, 2002)

Los 34 países miembros se reúnen regularmente para identificar problemas, discutirlos, analizarlos y promover políticas públicas que permitan resolverlos, bien sea por acuerdos internacionales o por la adopción de normativa interna para cada país.

Entre miembros y participantes de la OCDE se cuenta con el 80% de representación en el comercio mundial, además de las inversiones globales que encarnan en este organismo un papel fundamental para hacerle frente a la evolución de la economía y los mercados mundiales.

Una vez identificado el funcionamiento de la OCDE, se debe reseñar la importante intervención que ha tenido en el siglo XXI para ayudar a asegurar la privacidad y la protección de los datos personales contenidos en bases de datos o archivos físicos, electrónicos y en línea. Para este reto la operación de la OCDE se basa en tres principios orientadores que son: *democracia pluralista, respeto de los derechos humanos, y economías de mercado abierto* efectivos desde el 30 septiembre de 1980.

Los lineamientos dados en torno a la OCDE permite una cooperación y compromiso de los gobiernos para establecer soluciones armonizadas con cada ordenamiento jurídico, comprometiéndose a proteger la privacidad en el ámbito global, basada en una cooperación conjunta entre la empresa, la industria, los gobiernos y la sociedad civil, además de los países no pertenecientes a la OCDE y los demás organismos internacionales, anticipando, desde el discurso y la reflexión, el posible desarrollo tecnológico que pudiera afectar la privacidad y perfilando políticas exhaustivas y coherentes para la protección en pro del ciudadano.

1.4. Aproximación al Caso Norteamericano

Desde otro escenario es importante manifestar lo que paso en EEUU en cuestiones decantadas por diversos autores respecto a "el derecho de estar solo", por ejemplo dice (Cavero, 1993): "todo intento por delimitar el significado de «intimidad» parte con una dificultad previa: no existe –dice– un acuerdo generalizado sobre el término concreto a utilizar ni en la vida cotidiana ni entre los que estudian la cuestión", "Se emplean por igual las expresiones «intimidad», «vida privada», o «esfera privada», «ámbito íntimo»

o «privado», y la cada vez más común «privacidad», un neologismo que como los anteriores sirve para referirse a ese deseo de disfrutar lo personal y la pretensión consiguiente de exigir a los demás su respeto y, en su caso, su protección legal".

Tratamiento terminológico que no tiene necesariamente que ver con la posibilidad de utilizar nuestros datos personales para la finalidad determinada por la persona que los recolecta, marcándose la diferencia cuando se habla del derecho "a estar solo" el cual se refiere más exactamente al derecho de privacidad y de intimidad, mas no relacionado con los datos personales, que, si bien se refieren a una persona física, no necesariamente sean íntimos para que merezcan una protección.

Con la indicación de los escenarios Internacionales como algunos referentes históricos, Alemania Nazi, Unión Europea, OCDE y la Aproximación al Caso Norteamericano, NO se identifica que allí se agota la escenificación global en la materia, sin embargo, constituyen referentes históricos y contemporáneos mundiales cuando se involucran la discusión el tema de los datos personales en relación a su protección, privacidad, disponibilidad, tratamiento y circulación, admitiendo que es el inicio de una temática dinámica, cambiante y de proyección progresiva a partir de aspectos como el desarrollo tecnológico y la innovación con utilización de datos.

b) **Perspectiva Colombiana**

El artículo 15 de la Constitución Política Colombiana de 1991, definió sin limitaciones, el derecho a la protección de datos personales en asocio con el derecho a la intimidad personal como un derecho Constitucional, general, absoluto, patrimonial, inalienable, imprescriptible y que se puede hacer valer por cualquier ciudadano erga omnes[8] frente al Estado y a cualquier particular.

Es a partir de la Sentencia C-748 de 2011, por medio de la cual la Corte Constitucional declara la constitucionalidad del proyecto de ley estatutaria que da vida a la Ley 1581 de 2012, en la cual, dijo la corte que, toda persona

[8] Es un término aplicado en el lenguaje técnico jurídico para significar "frente a todos". Consultado en Diccionario Jurídico. Recuperado noviembre 2014. www.ic-abogados.com.

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[9], 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.

Es por ello que el titular de un dato personal, de acuerdo como está creada 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, la cual se entiende cómo:

> Atendiendo a lo que reza el art. 1741 C.C. indicando que se considera nulidad absoluta cuando falta algún requisito o formalidad que las leyes prescriben para el valor de ciertos actos o contratos en consideración a su naturaleza, en consecuencia un dato personal no tiene disponibilidad, toda vez que se vincula al ser, al sujeto físico como una características personalísima, en cuyo caso, solo puede replicarse de él para su reconocimiento y existencia, impidiendo que su titular pueda enajenarlo y liberarse de él, ello se traduciría que en cualquier sujeto físico puede liberarse de su personalidad jurídica, art. 14 Constitución Política de 1991, hecho imposible, ni aun estando muerto, pues la persona sigue reconociéndose en el ordenamiento jurídico colombiano ya no como un ser físico vivo, por el contrario como ciudadano fallecido.

Pudiendo afirmarse que su permisibilidad o disponibilidad frente a la reglamentación que dispone el ordenamiento jurídico colombiano, es inalienable e irrenunciable, inherente al ser humano y a su personalidad jurídica.

La protección del Dato Personal y la Intimidad, consagrada en el art. 15 C. Pol., 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", (Sentencia Constitucional, 2011)

[9] Primera referencia que interrelaciona la intimidad con la privacidad a partir de la protección al dato personal, la autorización y disponibilidad de éste por su titular respecto de la utilización que de él hagan terceros.

que tiene todo ciudadano respecto del tratamiento de sus datos en bases de datos, archivos, y bancos de datos, dando respuesta a la necesidad de establecer límites como lo indica el artículo 15 C. Pol. "la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución".

La ley 1581 de 2012 se expide para la protección de todos los Datos Personales a nivel general, salvo los que se someten a regímenes especiales como se identifican en el artículo 2 de la ley en atención a que su protección por un régimen especial sea coherente, claro, seguro y favorable de acuerdo a su naturaleza o su especial justificación legal de conservar o preservar otro tipo de protección, aun siendo un dato personal, así:

> Artículo 2°. Ámbito de aplicación. El régimen de protección de datos personales que se establece en la presente ley no será de aplicación: a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico. Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley; b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo; c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia; d) A las bases de datos y archivos de información periodística y otros contenidos editoriales; e) A las bases de datos y archivos regulados por la Ley 1266 de 2008; f) A las bases de datos y archivos regulados por la Ley 79 de 1993. Parágrafo. Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley.

Pese a lo anterior, en un mundo como el de hoy, digitalizado, donde los datos personales no solo se recogen directamente del individuo como resultado

del ejercicio de su personalidad jurídica[10], sino que también con captados en tiempo real por mecanismos tecnológicos como fueran, entre otros, los dispositivos móviles, plataformas web, sistemas de tratamiento de información, sensores desarrollados para la utilización de aparatos tecnológicos, e incluso captura de identificación de sentimientos y estimulación de una persona tiene frente a su entorno, es prioritaria la protección a la privacidad y la información, no solo a nivel nacional sino global, que permita caracterizar la sociedad Colombiana como garantista y democrática, además defensora de los Derechos Constitucionales, como es la Protección del Dato Personal.

1. Aproximación al alcance de la Protección ((DDI), 2014)

En Colombia es a cargo de la SIC[11] la protección y garantía del derecho de Habeas Data[12], al igual que la Protección del Dato Personal[13], el verdadero medio de defensa tiene que involucrar no solo al Estado sino también a su titular y a cada empresa recolectora del dato, exigiéndole en todo caso, que su facultad de recolección, tratamiento y circulación del dato, no responda a intereses individuales, sino legales que permita, al momento de la captura de datos, minimizar los riesgos de afectación al titular por la ejecutoria de conductas empresariales abusivas frente a los clientes, proveedores, y entidades estatales.

El acceso a su información y dato personal, a nivel global, sino está autorizado, puede considerarse un ilegítimo, máxime cuando este acceso constituye la posibilidad de utilización y apropiación de los archivos personales, imágenes, contraseñas de acceso a sitios que requieran autenticación personal, y la finalidad de quien los usa sea para ocasionar daños o uso mal intencionado, e incluso la afectación directa a múltiples facetas de la vida como son la reputación personal, la vida laboral y profesional, entre otras.

---

10 Art. 14 Constitución Política de Colombia 1991. Artículo 14. Toda persona tiene derecho al reconocimiento de su personalidad jurídica.

11 SIC: Superintendencia de Industria y Comercio de Colombia.

12 A cargo de la delegatura del Habeas Data. Consultado noviembre 2014. http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_conferencias_varsovia_2013_resol_dirreccion_estrategica.pdf.

13 A cargo de la delegatura de la Protección del Dato Personal. Consultado noviembre 2014. http://www.sic.gov.co/drupal/sobre-la-proteccion-de-datos-personales

En definitiva, la Protección del Dato Personal comporta una posibilidad de brindarle al ciudadano una herramienta jurídica y reglamentaria que le permita defender su Bienestar y evitar actos delictivos que se traduzcan en una suplantación de identidad por un tercero malicioso.

2. Caracterización del dato personal protegido

La Protección del Dato Personal y la identificación del dato en sí mismo consagrado en el art. 3 de la ley 1266 de 2008 y el desarrollo jurisprudencia que ha dado la Corte Constitucional en la materia, permite identificar que las características principales que posee el DP[14] y su protección, además que lo diferencian de otros derechos constitucionales como el Habeas Data, indicadas en la Sentencia C-748 de 2011, así:

> Las características de los datos personales son las siguientes: i) estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menos 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, y iv) su tratamiento está sometido a las reglas especiales (principios) en lo relativo a su captación, administración y divulgación.

Esta modelación de la protección del dato personal en Colombia da cumplimiento a la directriz de la OCDE (OCDE, 2002) sobre la protección de la privacidad y flujos transfronterizos de datos personales, en relación a la segunda sección de la directiva que establece los principios básicos para la aplicación en la normativa interna de cada nación en relación a la especificación del uso hacia el titular al momento de otorgar autorización del dato, las limitaciones del uso de éste y la salvaguardia que debe otorgársele. Es por ello que en la ley 1581 y decretos 1377 y 886, además de la circular 2, se regulariza aspectos relevantes para el tratamiento y circulación del dato como son: a. autorización previa del titular, b. prohibiciones frente a la disponibilidad del dato por parte del responsable y encargado, 3. Habilitación de tratamiento y circulación que no requiere previa autorización del titular,

[14] Dato Personal

4. Adopción de políticas, procesos y procedimientos de seguridad del dato personales en relación a riesgos de pérdida o acceso no autorizado, destrucción o alteración del mismo, divulgación o resguardo injustificado, entre otros.

Esta caracterización del dato pone una primera mirada sobre el que sucede frente a actos de investigación por hechos criminales, y la respuesta que parece apenas lógica es que el Estado sea de forma directa o por intermedio de entes técnico científicos que le cooperen puede acceder a los datos personales protegidos sin pedir autorización previa, pero que pasa entonces en obtenciones de datos sin previa autorización basados en procedimientos autorregulados o autonormados, e incluso cuando se trata de investigaciones preliminares que no se conoce previamente si constituye un acto delictual o no, tema que se tratará más adelante.

3. Principio de responsabilidad demostrada

La ley 1581 de 2012 y su decreto reglamentario 1377 de 2013 en su art. 26, desarrolla el principio de responsabilidad demostrada, que reza:

> Artículo 26. Demostración. Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto, en una manera que sea proporcional a lo siguiente:
>
> 1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.
>
> 2. La naturaleza de los datos personales objeto del tratamiento.
>
> 3. El tipo de Tratamiento.
>
> 4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.
>
> En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso.

> En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas

Plantea para toda persona que recolecte datos personales, una obligación en la adopción de programas integrales para el desarrollo de esa actividad, permitiendo dar cumplimiento al Derecho Fundamental de la protección constitucional y legal del dato personal a partir de la Constitución Política de 1991, como fuente de Derecho Fundamentales en doble vía de relación protegida, –entre el titular del dato personal y el recolector– sin llegar a deslegitimar, que se considera la protección como fundamental porque el dato, en sí mismo, es subsumido en consideración a su esencia.

El programa integral de protección de datos personales, no puede responder a estándares generalizados por sectores empresariales, en contrario, deben responder a un análisis e implementación del programa de protección de datos personales, hecho a la medida de la empresa, teniendo como consecuencia el desarrollo de un instrumento protector del cliente o proveedor, haciendo uso de su papel de titular del dato personal.

La consecuencia directa y más importante sobre esta adopción de un programa integral en protección de datos personales, es la confianza entre el comerciante y su cliente, que se traduce en sanciones al responsable o encargado que no cumpla con la medida (SIC, 2014), la cual no se ve materializada solo en el producto o servicio que le dispone, sino en la confianza sobre el manejo que da a su información personal, capital invaluable para el cliente final, permitiendo generar lazos fuertes e infranqueables respecto a su competidor comercial, aun enfrentándolo a estrategias económicas insuperables, pues un cliente que confía, es un cliente que nunca deba su proveedor, en un medio de mercado masivo desde entornos digitales y con captura en tiempo real de sus datos personales, permitiendo llegar a él de forma inmediata y ágil, a bajo costo y con estrategias innovadoras, impidiendo el acceso a otros proveedores del mercado.

La protección del dato personal a nivel mundial está diseñado para que la industria y el comercio, primero estén obligados a generar estrategias de recolección, tratamiento y circulación de datos, bajo una previa autorización "el permiso del titular", antes de proceder a su uso y conservación, pero no así es generalizado para las empresas el diseño de sus estrategias de mercado,

muchas de estas respondiendo a metodologías que no evidencian ni piensan en el permiso previo por parte del titular para la obtención de su dato personal, sobre las políticas de tratamiento, ni las medidas de seguridad y protección de sus datos, que navegan comercialmente en un escenario oculto sobre el tratamiento de sus datos, es un escenario de incertidumbre y desconfianza del cliente frente al comerciante e industria.

Si pensamos en el *goodwill* (Sentencia Good Will o Credito Mercantil, 2013) indicando la alta corte, que este activo intangible refleja las conexiones de un negocio en atención al cliente, la reputación y otros factores similares, permitiendo establecer un costo de enajenación de la empresa, en atención a que la reputación de la empresa es posible valorizarse, incluso reflejarse en la información contable. Es posible para la empresa que la política corporativa en el tratamiento de datos personales, donde le permitan al cliente el control directo sobre su dato, acreciente de forma significativa su buen nombre, fortaleza su confianza y reputación, en consecuencia, su valor comercial o crédito mercantil aumente significativamente, sin que ello se derive directamente el producto o servicio que prestan.

Referente a este respecto la OCDE (OCDE, 2002) en la directiva de protección de datos personales establece que la responsabilidad sobre la protección o no del dato recae exclusivamente en el "controlador del dato", en Colombia tanto para el Encargado como el Responsable del dato, reseñando que se encuentra en la obligación de establecer medidas de seguridad para su protección e identificación de incidentes que den cuenta de su violación, exigencia que abre el debate en relación a la Evidencia Digital, no cuando es dada a instancias del Estado, allí es claramente justificante, se centra más cuando su extracción es por entidades privadas o con fundamento a normas de autorregulación, por que dejan al arbitrio la protección excesiva del dato impidiendo la obtención de la prueba o la excesiva disponibilidad del dato que pone en riesgo un Derecho Constitucional existente por él y para el ciudadano mundial.

La protección al dato personal en relación con la responsabilidad demostrada, es dar un reflejo de compromiso económico entre la empresa y las entidades para sus clientes, permitiendo al Estado Colombiano hacer gala de la protección a la privacidad y el dato personal materializado en las buenas prácticas que acogen en cuanto a la recolección, tratamiento y circulación, siempre en perspectiva de protección que no solo las normas

legales como ha sido la expedición de la ley 1273 de 2009 o ley de delitos informáticos incluyendo el tipo penal de violación de datos personales, además la conjugación con las normas de carácter administrativo y reglamentario al interior de toda organización.

La SIC a través de la Delegatura de Datos Personales, acoge las guías internacionales para el tratamiento de DP, encaminados a proteger la privacidad de los ciudadanos de forma global y en consecuencia establecer flujos fronterizos de información de manera segura y confiable.

Finalmente, la OCDE determina a los gobiernos que la implementación de la norma al interior se debe establecer de cara a que las empresas y organizaciones puedan demostrar su cumplimiento desde la implementación, ejecución, revisión y mejoramiento continuo. En Colombia, al emitirse la Guía de Responsabilidad demostrada se fomenta la autorregulación de la entidad, quien a su vez es obligada a dar cumplimiento a dar protección al dato personal. La autorregulación se materializa a través de protocolos de calidad, forenses digitales, seguridad de la información, entre otros.

II. Mirada a la privacidad, intimidad y dato personal en relación

Estas figuras representativas de derechos personalísimos y responsabilidades empresariales y Estatales, merecen su individualización en procura de establecer su alcance y límites de aplicación y protección.

Se debe partir desde el concepto de lo público, con el fin de delimitar hasta dónde puede llegar el Estado en la invasión de la espera personal del sujeto físico sobre el conocimiento de su vida privada, que generalmente en los Estados con perfil social y de derecho, la categoría de privacidad o publicidad de una persona es dada por su relación con el Estado, caso en el cual se considera un ciudadano políticamente expuesto o una persona va a depender de su función con relación al Estado se considera entonces un ciudadano en calidad de funcionario público, puede afirmarse que tiene una privacidad más limitada mirado en correlación con un ciudadano que trabaja en una empresa privada, el cual tiene un espectro mucho más amplio en la esfera de lo protegido, constituyendo un límite del hasta dónde puede llegar el Estado.

Cabe preguntarse, en relación a la función pública, ¿cómo puede delimitarse la esfera de lo privado y la intimidad?, la respuesta es ambigua,

teniendo en cuenta que la esfera de lo privado merece el mayor resguardo, y es lo que constituye la esfera de lo íntimo que está relacionado con aspectos que puedan declararse, no en función de ser un ciudadano políticamente expuesto o funcionario público, sino en función de los pensamientos, los sentimientos, la vida absolutamente íntima de una persona en cuanto qué piensa, qué siente, qué hace adentro de su casa, qué hace cuando comparte su vida sexual con otra persona, qué hace cuando comparte su ideología política, qué opina de determinadas cosas, de dónde viene, cuál es su origen étnico, qué religión profesa si es que lo hace.

Desde la esfera absolutamente resguardada, en la cual nadie puede llegar "el derecho a estar solo" tiene que ver más con la espera de lo íntimo que con la espera de lo privado, en atención a que el sujeto físico, en la espera de lo privado tiene derecho a estar solo hasta que el Estado pueda indagar y en algunos casos exigir que declare públicamente, como sería tomada la consecuencia de ser citado como testigo en un proceso judicial.

Así las cosas, existe una barrera más permeable la distinción entre lo privado y lo público, y una barrera mucho más fortalecida entre la distinción entre lo íntimo y lo privado, y en lo íntimo no puede el Estado no puede tener injerencia de ninguna manera, a diferencia de lo privado que se justifica a partir de situaciones particulares donde el Estado si puede tener injerencia, escenario que permite ver que el ámbito de los datos personales también tiene en cuenta, al establecer la esfera de protección, respecto del gasto, y cuando constituye un ámbito íntimo y un privado, criterio éste que no se encuentra de forma explícita en la mayoría de las legislaciones donde se proteja el dato personal, pero si a partir de una construcción teórica o doctrinaria con fundamento al uso de la interpretación jurídica al bloque de constitucionalidad.

Cuando ambos términos son utilizados como si fueran sinónimos, sin que ello sea real puesto que abarcan cuestiones, toma de nuevo importancia respecto al otro escenario que constituye la materia de protección de datos personales, los cuales a su vez se clasifican en Colombia a partir de la Ley 1266 de 2008 en su artículo 3, como públicos, semiprivados y privados, en concordancia con la Ley 1581 de 2012 artículo 5, el cual indica lo que debe entenderse como dato sensible (salud, educación, política, preferencia sexual, religión, raza, entre otros), que en principio se protegen a partir del alcance a la

intimidad, sin embargo, se puede establecer en qué casos una persona natural o jurídica, o el Estado puede satisfacer con la apertura de la información intima la cual es propia del ciudadano o único dueño.

En referencia a la protección de datos personales es otro escenario normativo, donde existen requisitos a cumplir por el Estado para recolectar datos personales y fundamentalmente los particulares. Cuando apunta al Estado en ejercicio de su función pública que debe poder recaudar información personal y acumular esa información personal de una determinada manera, se establece éste ¿qué debe hacer? y ¿qué debe garantizar?, siendo en principio destacable garantizar que los ciudadanos pueden estar tranquilos sobre su información no va a ser utilizada para fines totalmente distintos a los que fueron creados.

Después de la época del Tercer Reich, de la segunda guerra mundial, lo que ocurrió en la sociedad a nivel global era una necesidad de legislar respecto a la acumulación de datos y la manera en que se tenía que proteger para que no pudieran ser utilizados con una finalidad distintas a las que fueron creadas, ahí es donde surge todo lo que tiene que ver con el derecho a la protección de datos personales, ello se evidencia en tratados internacionales sobre la protección de derechos humanos DDHH.

En atención a este reconocimiento es que ahora se reconoce la situación de la persona física, fuente generadora de datos personales, incluso desde el momento de su concepción, desde el momento en que a la madre se le decreta su estado de gravidez, los cuales se van acumulando a lo largo de la historia de la persona, teniendo una relevancia tal, por su volumen de información vinculada que, en el mercado de venta de bases de datos, también pasan a tener un valor económico.

El principal recolector de datos es fundamentalmente el Estado a través de distintas herramientas, instituciones y finalidades, ejemplos de ellos son los recolectados como datos clínicos que se conocen a partir la concepción del feto, posteriormente datos de nacimiento en el momento del parto, los recolectados en el momento de la matrícula académica desde el jardín hasta los estudios posgrado, igualmente los recolectados durante las prácticas académicas, universitarias, laborales o como trabajador independiente, igualmente datos que corresponden al patrimonio.

Entidades del Estado recolectoras de datos personales, son entre otras, la registraduría del Estado Civil, el registro RUNT para el Ministerio de

Transporte y Tránsito, el registro del RUT para servicio de la DIAN. Ésta última entidad, decide sistematizarse con la implementación del programa MUISCA, bases de datos recolectadas que permiten lograr al Estado a través de los fines de la entidad, entre otros logros "los que apuntan a un mejoramiento del recaudo, de la gestión y al posicionamiento de la DIAN, tanto en el corto como en el largo plazo" [15].

Es por ello que el Estado cuando quiere cruzar nuestros datos recolectados, tiene a su disposición cualquier cantidad de información vinculada al ciudadano, como ya se indicó, desde su concepción, estudio, trabajo, salud, al momento del voto, fuente a su vez generadora de datos en categoría sensible, quizás los de mayor necesidad de protección, siendo importante la concientización generalizada del ciudadano, las organizaciones y el Estado en materia de la protección dada a los datos personales que se van acumulando, para poder resguardar derechos que son de mucha mayor jerarquía como lo son el derecho a la intimidad y la privacidad.

III. Evidencia digital

1. Breve mirada internacional

Es un campo que determina el escenario que rodea la Evidencia Digital, a partir de protocolos forenses certificados por instituciones reconocidas, además de los estándares aplicables a laboratorios forenses y el perito forense, permiten dar respuesta a las necesidades investigativas en las nuevas formas delictuales o cibercriminales, cumpliendo requisitos de legalidad y legitimidad tanto de la evidencia como de la prueba, por la utilización de protocolos certificados y de reconocimiento internacional, aunque de gran costo en su adopción al caso concreto.

Lo anterior tiene como efecto principal, que los actos investigativos se direccionan para extraer una evidencia digital, al momento de la investigación del delito informático, como es el caso colombiano o de países latinoamericanos, el aval a la evidencia realizada a partir de la certificación del instituto como fuente de respaldo en el cumplimiento de autenticidad, integridad, originalidad, confiabilidad y no repudio.

[15] http://www.dian.gov.co/content/muisca/muisca.htm Consultado 3 noviembre de 2014.

Los institutos más importantes, SANS[16] y el NIST[17], de ello se indicó (Elneser, 2013):

> El interés del instituto es la difusión y cooperación en las técnicas y protocolos forenses aplicables en caso de delitos informáticos y los demás que involucren la aplicación de herramientas informáticas, con la finalidad de ayudar a los investigadores certificados, poniendo a disposición de forma gratuita documentos de investigación científica en el campo de la seguridad de la información y en los aspectos que involucran la informática forense y el derecho informático, temáticas que nutren el contexto total del campo de la investigación forense digital para la obtención de evidencia digital, con la aplicación de protocolo y herramientas forenses, no solo las consideradas por certificadas por un instituto reconocido como es SANS, sino también que permiten la obtención de la evidencia digital con características de autenticidad, integridad, originalidad, confiabilidad y no repudio.

En igual perspectiva frente a la utilidad y respaldo dado a la Evidencia Digital, se cuenta con el NIST (Elneser, 2013):

> Para el campo de la informática o computación forense promueve programas académicos de contenido novedoso y contemporáneo, satisfaciendo los retos diarios que la ciberdelincuencia plantea, entre los cuales podemos encontrar: Educación Nacional de Seguridad Cibernética de la Iniciativa (Niza), Biblioteca Nacional de referencia de Software es un proyecto apoyado por el Departamento de Justicia Estadounidense adscrita al Instituto Nacional de Justicia Federal, el Estado y Policía Local, además del National Institute of Standards y Tecnología-NIST, y las organizaciones de la industria para revisar los archivos de las computadoras, se puede definir esta cooperación como la forma eficiente y eficaz de usar tecnología informática "haciendo

16 SYSADMIN AUDIT, NETWORKING AND SECURITY INSTITUTE. Institución con ánimo de lucro fundada en 1989. Dedicada a la formación, entrenamiento y certificación de profesionales en Seguridad Informática. Con sede en Bethesda (Maryland, Estados Unidos). https://www.sans.org/

17 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Es una agencia de administración de tecnología promoviendo la innovación y competencia industrial mediante avances en metrología, normas y tecnología que mejoren la estabilidad económica y la calidad de vida. Creada desde 1901. ubicada en Gaithersburgo, Maryland. http://www.nist.gov/

coincidir perfil de los archivos en el RDS, Esto ayudará a aliviar gran parte del esfuerzo necesario para determinar qué archivos son importantes como pruebas en los equipos o sistemas de archivos han sido incautados en el marco de las investigaciones penales" (NIST - National Institute of standards and technology), por ello se constituye como biblioteca dedicada al almacenaje de los tipos de software, Equipos forenses y referencia datos (CFReDS), permitiendo el desarrollo de equipos forenses de referencia Data Sets (CFReDS) para pruebas digitales.

Ambos institutos han establecido un escenario mundial que garantiza la ejecución de actos de investigación con fundamento a la preservación de la privacidad, la intimidad y la protección del dato personal, respecto de lo recolectado en una prueba forense, en atención a los protocolos forenses digitales que administran y tienen estandarizados, permitiendo esclarecer los hechos sin que el presunto sindicado, sea violentado en sus garantías constitucionales, ya que en atención a las normas legales, ellas en sí mismas poseen falencias en la sistemática, en la recogida de elementos, piezas y objetos de convicción, por tanto, debe respetar un doble filtro, pasando inicialmente por las indicaciones legales del procesamiento y procedimiento sobre la etapa de actos de investigación y finalmente la etapa de actos de prueba.

La OCDE a partir de normas en países miembros u otros, identifica lineamientos uniformes en materia de la evidencia digital, disponiendo que ésta debe ser extraída adoptando un protocolo que respete los derechos fundamentales de los ciudadanos, en contrario sería constitutiva de violación de un derecho fundamental.

En los lineamientos generales de política dada a instancias de la OCDE (OCDE, 2002) se indica que debe considerarse fundamental que la extracción de una evidencia digital debe darse en el marco de: *a. limitación del uso dado en la autorización, b. salvaguardar la protección del dato personal contentivo en la extracción* como requerimientos fundamentales que evidencian la protección del dato personal.

Si bien, en la directiva no se habla de la evidencia digital de forma directa, entender cada una de las figuras de efectos legales permite hacer transversalidad y establecer que la extracción de la evidencia digital realizada por parte del gobierno es absolutamente legítima y actúa como eximente de violación a la protección de dato personal, por ejemplo, en Colombia se

amparado desde el art. 15 de la constitución política de 1991 y del art. 10 de la ley 1581 de 2012, de modo contrario se puede concluir sobre la extracción de la evidencia digital realizada por un ente privado en cumplimiento de un contrato para la extracción de la evidencia digital, o como parte del protocolo interno en la atención de incidentes informáticos.

2. Breve mirada nacional

Inicialmente hay que delimitar que el término jurídico de la evidencia digital en Colombia no se encuentra expresa en el ordenamiento jurídico en general y que a su vez en el art. 275 de la Ley 906 de 2004, solo se tienen las categorías correspondientes a medios cognitivos, las denominadas Evidencias Físicas y Elemento Material Probatorio, permitiendo concluir que la podemos entender como: la evidencia construida por campos magnéticos y cursos electrónicos, que puede ser reportada, almacenada y realizada con herramientas técnicas específicas, entiéndanse protocolos, software y hardware vinculado, que no se han desarrollado para el Estado Colombiano a la medida, por consiguiente, se han acogido las internacionales del NIST y del SANS principalmente.

Igualmente el ámbito privado participa en los actos de investigación e indagación, reconociendo su intervención en calidad de *Órgano Técnico – Científico* art. 204 C.P.P., legitimado en un principio denominado, *libertad de la prueba* art. 373 y 380 C.P.P., que admite la utilización de protocolos, laboratorios y peritos forenses certificados, siempre y cuando su actuar se ejecute respetando los derechos humanos consagrados para el ciudadano desde la promulgación de la Constitución Política de 1991, los cuales disponen *"las excepciones y limitaciones jurídicas, el nuevo medio de prueba que pretende hacerse valer en el proceso no puede utilizarse sino cuando los respete"* (Comisión Interinstitucional para la Implementqación del Sistema Acusatorio, 2005).

Partiendo de este escenario Público-Privado en materia de investigación criminal para Colombia, se hace necesario un análisis reflexivo en cuanto a los protocolos de investigación forense aplicables en la obtención de la evidencia digital, la cual a su vez no se encuentra regulada de forma expresa en el Código Procesal Penal, art. 275:

> "Elementos materiales probatorios y evidencia física. Para efectos de este código se entiende por elementos materiales probatorios y evidencia física, los siguientes: g) El mensaje de datos, como el intercambio electrónico de datos, internet, correo electrónico, telegrama, télex, telefax o similar, regulados por la Ley 527 de 1999 o las normas que la sustituyan, adicionen o reformen; h) Los demás elementos materiales similares a los anteriores y que son descubiertos, recogidos y custodiados por el Fiscal General o por el fiscal directamente o por conducto de servidores de policía judicial o de peritos del Instituto Nacional de Medicina Legal y Ciencias Forenses, o de laboratorios aceptados oficialmente.

Por el contrario, su obtención responde a estándares de calidad emitidos y certificados por entidades u organismos del ámbito privado, nacional e internacional, siendo los más relevantes ISO, SANS y NIST.

Para Colombia se cuenta con ICONTEC desde 1963, entidad que hace parte de IQNet[18], lo que permite darle un alcance internacional a las certificaciones que ellos expiden en países donde se encuentran organismos de igual operatividad[19]. Entre los servicios que posee se tiene la implementación, capacitación y formación, además de evaluación para certificación y re-certificación en el cumplimiento de implementación en una norma ISO son producto de la auto-regulación de organismos y empresas privadas, sin que previamente exista delegación por parte del Estado de esta función pública adscrita al Poder Judicial, constituyendo, a mi juicio, un indicador de pérdida de soberanía y control del Estado, al momento de regular los actos de investigación e indagación por entes públicos, toda vez que son normas que no se someten a control de legalidad, además quien determina su validez y eficacia jurídica, particularmente que no sea violatorias de la ley y la constitución, como si lo

---

18 Red mundial de los principales Organismo de Certificación

19 AENOR Spain, AFNOR France, AIB Belgium, ANCE México, APCER Portugal, CCC Nicosia, CISQ Italy, CQC China, CQM China, CQS Czech Republic, CRO CERT Croatia, DQS Germany, FCAV Brazil, FONDONORMA Venezuela, ICONTEC Colombia, IMNC Mexico, IRAM Argentina, JQA Japan, KFQ Korea, MIRTEC Greece, MSZT Hungary, NEMKO Norway, NSAI Ireland, PCBC Poland, QUALITY Austria, RUSSIAN REGISTER Russia, SII Israel, SIQ Slovenia, SIRIM Malasya, SQS Switzerland, SRAC Romania, TEST-St. Petersburg Co. Ltd. Russia, TSE Turkey y YUQS Serbia. 2014. Recuperado de http://icontec.org/index.php/es/nuestra-compania/nuestra-compania/reconocimientos-internacional.

tiene el Código Penal[20], Procesal Penal[21] y el Estatuto Orgánico de la Fiscalía General de la Nación[22].

Para el ámbito en que se enmarca la temática del presente escrito, los protocolos básicos para evidencia digital, se cuenta con el servicio de certificación y re-certificación en el cumplimiento de normas ISO, como son:

- NTC ISO 17025: Identificación de brechas entre lo desarrollado por la organización y los requisitos establecidos en los esquemas de acreditación en la norma. Es una herramienta que ayuda a la dirección, en la medida que evalúa de una manera relativamente independiente el sistema de organización y administración de laboratorios y organismos de inspección. Facilita una evaluación global y objetiva de los inconvenientes de la empresa, que generalmente suelen ser interpretados de una manera parcial por los procesos afectados. Detecta si las actividades se llevan a cabo conforme a lo estipulado en los procedimientos, instrucciones o normas. Identifica documentos desactualizados que ya no reflejan la práctica actual. Mejora la comunicación interna. Asegura que la dirección conoce la situación del sistema de calidad, sus fortalezas y debilidades (ICONTEC, s.f.).
- NTC ISO IEC 27001 – 2013: Tecnología de la información. técnicas de seguridad. sistemas de gestión de la seguridad de la información (SGSI). Requisitos. La NTC-ISO/IEC 27001 fue ratificada por el Consejo Directivo del 2006-03-22. Esta norma cubre todo tipo de organizaciones (por ejemplo: empresas comerciales, agencias gubernamentales, organizaciones sin ánimo de lucro). Esta norma específica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos globales del negocio de la organización. Especifica los requisitos para la implementación de controles de seguridad adaptados a las necesidades de las organizaciones individuales o a partes de ellas. El SGSI está diseñado para asegurar controles de seguridad suficientes y proporcionales que protejan los activos de información y brinden confianza a las partes interesadas.

20 Ley 599 de 2000 reformado por la Ley 1273 de 2009.
21 Ley 906 de 2004.
22 Ley 938 de 2004.

- ISO/IEC 27037:2012: "Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence" viene a renovar a las ya antiguas directrices RFC 3227 estando las recomendaciones de la ISO 27037 más dirigidas a dispositivos actuales y están más de acorde con el estado de la técnica actual. Esta norma está claramente orientada al procedimiento de la actuación pericial en el escenario de la recogida, identificación y secuestro de la evidencia digital, no entra en la fase de Análisis de la evidencia. Las tipologías de dispositivos y entornos tratados en la norma son los siguientes: a. Equipos y medios de almacenamiento y dispositivos periféricos. b. Sistemas críticos (alta exigencia de disponibilidad). c. Ordenadores y dispositivos conectados en red. d. Dispositivos móviles. y e. Sistema de circuito cerrado de televisión digital (Perito IT, 2012).

Recientemente se ha proyectado el mejoramiento en la normalización de la Evidencia Digital a través de un estándar británico, proponiendo una mejor calidad en los procesos y procedimientos ya existentes en protocolos publicados por la ISO (ISO, 2014), sin embargo, su publicación no será de aplicación internacional salvo que los países adscritos a la ISO la adopten como norma autoreguladora.

Tanto los protocolos antes reseñados como éste último, denota que la función investigativa en materia de evidencia digital, acoge elementos de estandarización con una principal finalidad la cual puede resumirse, a mi juicio, en obtener evidencia basada en protocolos con certificación, permitiendo la presentación en juicio cumpliendo principios básicos en materia de producción y en especial admisibilidad de pruebas digitales ante el juez.

Cabe señalar que los requisitos legales pueden diferir extensamente en diversas jurisdicciones de todo el mundo. La premisa no es abogar por un criterio específico legal y universal en materia de tratamiento de sistemas informáticos, sino más bien a tener en cuenta los requisitos genéricos en cuanto a las cuestiones jurídicas que pueden ser adoptadas por cualquier el sistema legal, dependiendo los principios y derechos fundamentales reconocidos en el derecho interno o particular.

En materia de EVIDENCIA DIGITAL debe tenerse en consideración y cuidado cuando se aplican normas ISO en aspectos básicos de exigencia mundial:

1. Eliminación segura de los datos de pruebas y de caso al final del proceso judicial, en caso de ser ordenado por el Juez,
2. La conservación segura de los medios de comunicación y dispositivos de sujeción de la evidencia digital potencial como medida de lo posible,
3. conservación segura de la propia evidencia digital y la conservación segura de los resultados de la investigación para una posible futura referencia, y
4. Informe Pericial de los resultados de la investigación.

La admisibilidad de evidencia digital y de la opinión de expertos en un juicio, parten de la interpretación que de ello haga el fiscal a cargo del caso, luego el juez control de garantías y finalmente el juez de conocimiento, en estos casos la forma de analizar su admisibilidad responde a dos cuestiones en relación con la norma. En materia de la admisibilidad a un testigo técnico, este debe ser capaz de testificar sobre cómo fue adquirida prueba, como la conservo en laboratorio, además de dar cuenta frente al tratamiento, integridad y originalidad, aspectos prevalentes para hacer frente a la idoneidad de los procesos sin que emerja la necesidad de la calificación de otro experto en la materia, como lo plantea la norma ISO / IEC 27042, el perito experto podría dar fe de los hechos técnicos[23] aplicados.

Aunque los requisitos de admisibilidad varían entre las jurisdicciones, debe ser un criterio universal que incluyan por lo menos, lo siguiente en sus requisitos de admisibilidad de la evidencia Digital:

- Relevancia: la evidencia digital debe ser relevante para llevar al juez a la íntima convicción de los hechos y pueda fallar en derecho.
- La autenticidad: la evidencia digital debe demostrar que es lo que pretende ser, fuente o medio de prueba en sus diferentes modalidades o representaciones, como por ejemplo ser una Imagen JPEG extraído del disco duro de un servidor o un video extraído de un dispositivo móvil, en cualquier caso se presente el protocolo aplicado que respalda no se haya modificado de ninguna manera durante su recolección y extracción colección, en conclusión que el proceso de utilizado para extraer la imagen JPEG es digno de confianza, la cual se obtiene principalmente por el respaldo de instituciones como se considera a nivel internacional ISO.

[23] No se asimila a la fe pública que se relega sólo al Notario y Revisor Fiscal, en Colombia.

3. Evidencia digital en relación con intimidad, privacidad y datos personales en *log* [24]

Cuando se habla de un tratamiento del incidente informático se tiene que establecer el alcance de la intimidad y la privacidad desde dos miradas, o mejor desde dos disciplinas científicas que son el Derecho y Forense digital.

Cuando hablamos de incidente informático, tenemos en cuenta que se involucra no solo información, en muchos casos da cuenta de datos personales, contenidos en logs[25]. Para delimitar si la prueba pericial tiene relación o no con la privacidad, es necesario identificar si el incidente informático ha ocurrido, en una red pública o una red privada[26].

Por la naturaleza de lo establecido como log, es de uso privado, sin embargo, existe empresas dedicadas al ámbito estadístico, el cual solo es posible a partir de la información y datos recolectados. La recolección que realizan estas empresas se obtiene a partir del monitoreo de los puntos de acceso central a internet a los países para sacar información de navegación en la internet, sin o con permiso del titular de la información y del dato personal.

En materia probatoria, especialmente el ámbito penal, se categoriza, por doctrinal y análisis normativo, que la obtención de los log hace parte

---

24 Archivo que registra movimientos y actividades de un determinado programa (log file). En un servidor web, se encarga de guardar todos los requerimientos ("requests") y servicios entregados desde él, por lo que es la base del software de estadísticas de visitas. Consultado 3 noviembre 2014. http://www.lawebdelprogramador.com/diccionario/mostrar.php?letra=L&page=4

25 Archivo que registra movimientos y actividades de un determinado programa (log file). En un servidor web, se encarga de guardar todos los requerimientos ("requests") y servicios entregados desde él, por lo que es la base del software de estadísticas de visitas. Consultado marzo 2014. http://www.lawebdelprogramador.com/diccionario/buscar.php?opc=1&charSearch=log

26 La estructura de direccionamiento IP hace posible que los ordenadores se localicen entre ellos y puedan intercambiar información. Una dirección pública es una IP que se asigna a cada ordenador que se conecta a Internet, mientras que las privadas se usan para distinguir ordenadores dentro de una LAN corporativa o interna de una organización. Consultado marzo 2014. http://www.ordenadores-y-portatiles.com/ip-publica-privada.html.

de los actos de investigación, al respecto señaló la Corte Constitucional en sentencia C-396 de 2007:

> Es fundamental distinguir los actos de investigación y los actos de prueba. Los primeros tienen como finalidad recaudar y obtener las evidencias o los elementos materiales probatorios que serán utilizados en el juicio oral para verificar las proposiciones de las partes y el Ministerio Público y, para justificar, con grado de probabilidad, las decisiones que corresponden al juez de control de garantía en las etapas preliminares del procedimiento. En otras palabras, los actos de investigación se adelantan por la Fiscalía, la Defensa, el Ministerio Público y la víctima con el control y vigilancia del juez de control de garantías.

Por ello, la etapa que se surte para el desarrollo de los actos de investigación, sean dados por la fiscalía o por investigación privada, es en sí misma, un escenario de recolección de la información que dé cuenta del delito. De allí, que se pueda denominarse, una solicitud de log a los ISP[27] o las empresas de servicio en correo, redes sociales, sitios web, entre otros, como son, sin limitarse a ellas, Facebook, Yahoo, Gmail, Terra, actos de investigación, los cuales, dependiendo de su naturaleza y disponibilidad requieren o no un control previo o posterior de legalidad y legitimidad ante el juez.

Las empresas y los prestadores de Internet, han adoptado procedimientos legales uniformes para que los funcionarios judiciales y entes investigadores tengan conocimiento de cómo debe solicitarse la extracción del log, procedimientos que se desarrollan a partir de la política de privacidad, la cual, se encuentra en constante dinamismo, sea por el cambio de las estrategias comerciales, o sea por dar cumplimiento a la protección del dato personal.

Se hace necesario que la solicitud para la obtención de un log medie Juez Control de Garantías de forma directa o con la copia del auto que ordena la práctica del acto de investigación (extracción del log), se tramite por el interesado directamente frente a la embajada local con solicitud debidamente apostillada, especialmente cuando se tramita dentro del mismo país de ubicación de la empresa o del record keeper para la obtención del log. Dicha

27 Proveedor de servicio de Internet

extracción así presentada se obtiene de forma legítima y legal como medio cognitivo[28], posteriormente permitiendo su aportación a juicio como Prueba.

En ambos casos, se materializa el control de legalidad a través de una verificación del procedimiento de extracción de los logs dada, bien sea, por el propio servidor donde están alojados, mediando una autorización judicial o petición escrita y apostillada apelando al principio de libertad probatoria en el ámbito de la investigación privada.

Otra forma de hacer requerimiento a los record keepers es haciendo la petición apostillada para ellos directamente o pagando un abogado directamente en la zona de ubicación del servidor, de donde se hará la extracción del log con la finalidad de obtenerlo de forma legal.

El requerimiento también puede realizarse a EEUU a través de los corresponsables comerciales de cada empresa prestadora del servicio[29] para que, desde la sede oficial, sea ésta la que atienda el requerimiento, siempre y cuando el peticionario sea un forense digital certificado o la persona, sea natural o jurídica, interesada en la evidencia o material probatorio, en cuyos casos es a costos del peticionante.

Los procedimientos tramitados solo por intermedio del proceso ante Juez Control de Garantías, tiene duración de un año más o menos, teniendo en cuenta el trámite y legitimación de la actuación judicial, además del trámite por comisión que el mismo juez debe decretar para la embajada donde se requiera hacer la extracción, situación de tiempo que se puede minimizar, cuando quien solicita el acto investigativo, una vez el juez emita el auto que ordena la extracción, envíe directamente al record keeper el auto apostillado debidamente registrado para su trámite legal.

Igualmente, este requerimiento de la solicitud de log se puede realizar a través de la policía, la cual requiere o da traslado a la petición a través de la embajada, o directamente sobre Interpol[30], o directamente entre departamentos

---

28 Elemento material probatorio y evidencia física

29 ISO, YAHOO, GOOGLE, GMAIL, HOTMAIL, FACEBOOK, SKYPE, entre otros.

30 Con 190 países miembros, INTERPOL es la mayor organización policial internacional del mundo. Nuestra función consiste en permitir que las policías de todo el planeta colaboren para hacer del mundo un lugar más seguro. Nuestra moderna infraestructura de apoyo técnico y operativo contribuye a hacer frente a las crecientes dificultades

de policías de cada país cuando existen acuerdos internacionales de cooperación suscritos, con los cuales se le hace frente a la criminalidad.

La extracción del log se hace a través de la labor desplegada por el record keeper[31] (Peggy Valcke, 2012), para poder hacer la entrega de los logs solicitados a las entidades que están a cargo del servicio prestado en Internet, y que estos logs se encuentren relacionados con la investigación de un caso, preservando así los Derechos Constitucionales como lo son la privacidad y la intimidad, toda vez que este profesional aplique metodologías certificadas para la extracción.

Los logs de acceso también se almacenan, aparte de los servidores de los ISP, se replican a modo de respaldo en Google, siempre y cuando la página web este utilizando "Google AdWords"[32] se envía una copia de todos los logs a fin de que la herramienta pueda hacer el análisis y procesamiento estadístico de las transacciones en la página web consultada, como consecuencia emita los reportes de acceso.

Conclusiones

La creación de programas integrales de protección de datos personales a los que hacen referencia, tanto las guías de la OECD (Development, 2014) como las normas Colombianas, no se consideran una aplicación y uso restrictivo para la gran empresa, son procesos para cualquier empresa, escalables, que se deben hacer a la medida de cada organización que en su operación empresarial y comercial haga tratamiento de datos personales, obligando a repensar la manera de integrar procesos de análisis de información local y ahora nacional, igualmente a las entidades del Estado responsables de la supervisión, se deben

que comporta la lucha contra la delincuencia en el siglo XXI. Consultado marzo 2014 http://www.interpol.int/es/

31 Es la denominación dada al custodio o guardador de datos y registro en un sistema informático.

32 Permite que los clientes vean su empresa mientras buscan lo que ofrece en Google. Además, sólo se le cobrará cuando hagan clic en su anuncio para visitar su sitio web o llamarlo. Si no lo visitan, no paga. Registrarse en Google AdWords es gratis. Sólo paga cuando alguien hace clic en su anuncio para visitar su sitio web o lo llama. Es decir, cuando su publicidad es exitosa. Consultado marzo 2014. http://www.google.com.co/adwords/?channel=ha&subid=co-es-ha-aw-brh-2~64493853415

repensar en su forma de operar y el direccionamiento de las políticas públicas, para dar respuesta a las necesidades nacionales y trasnacionales en materia de protección a la privacidad, enfrentando retos del presente siglo como es el denominado el BIG DATA[33].

Todo modelo y metodología para la recolección, tratamiento y circulación de los datos personales aplicado por el Estado, o la empresa o el comerciante, tienen, indefectiblemente, que estar diseñados para dar respuesta a la protección del dato personal como derecho constitucional fundamental y exigido por los titulares de su información personal, que empoderándose de ésta pueden delimitar el uso y goce que de ellos hacen terceras personas con las que tenga relación directa e indirecta. De éste diseño a la medida se fundamenta la Responsabilidad Demostrada, exigible por la SIC a través de la delegatura de protección de datos personales, cuando realiza un proceso de inspección al cumplimiento de la normatividad en la materia.

Para preservar la privacidad de los logs y a su vez la conservación como fuente de información para probar el hecho delictivo, se puede solicitar a los ISP de transito de datos, como pudieran ser en Colombia Telmex, Une, Edatel entre otros, guardan logs de estadísticas de acceso de las empresas a las cuales les prestan el servicio, y con fundamento a los acuerdos suscritos para la protección de la propiedad intelectual directamente con la DMCA[34], ha obligado que los ISP filtren el tráfico de bittorrent[35], por ello, para la obtención de log sin depender del trámite por vía judicial, se puede consultar los acuerdos firmados del ISP en procura de la preservación y protección de los derechos de autor ante la DMCA y dependiendo del nivel de privacidad podrá habilitarse la solicitud del log directamente a la empresa, eso sí, en este escenario igualmente la persona encargada de la extracción es el record keeper.

La recolección de datos personales no es solo la respuesta a una necesidad de información, no opera solo como insumo para formular políticas públicas,

---

33 La ciencia del dato en masa, o conjuntos de datos no estructurados.

34 (Digital Millennium Copyright Act.) DMCA Título I: Ley sobre la implementación del Tratado de la OMPI sobre Derecho de Autor y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas. Año 1966. Consultado abril 2014. http://www.wipo.int/portal/es/

35 Protocolo de intercambio de archivos grandes o de punto a punto.

alianzas entre Estados y/o empresarios, es a su vez una fuente innegable de poder de la información, permea uno de los escenarios puestos en permanente revisión en todo lo que está significando la seguridad de la información tales como el acceso a los datos e información de cualquier calidad, uso, goce y masificación, sea o no autorizada, que en un principio se enmarcan en el mundo de la licitud y del ejercicio meramente de la función pública o estrategias de mercado, pasando a convertirse, por la ausencia de autorización previa, en recolección, tratamiento y circulación, violatorias de la protección del dato personal a cargo de la persona natural o jurídica que las ha recolectado.

La recolección, tratamiento y circulación del dato personal, núcleo central de la protección como respuesta a la responsabilidad empresarial, encuentra, ante la extracción de la evidencia digital dada sobre partes, componentes lógicos, sistemas de tratamiento de información, bases de datos y archivos, un eximente responsabilidad en los términos del art. 27 del decreto 1377 de 2013, por cuanto la extracción constituye precisamente un mecanismo mediante el cual se obtiene la información y datos, sean o no de carácter personal, almacenados en equipos computacionales o similares, y no por ello, la disposición que se haga de los datos personales será constitutiva de violación al derecho fundamental de protección del dato personal, puesto que la extracción valida la necesidad de la fuente de prueba, dando respuesta a la necesidad de recabar los rastros y evidencias existentes en los dispositivos contentivos de la información y datos personales, siendo imposible, previamente, exclusión de los archivos analizados.

La ponderación sobre valoración y defensa a Derechos Fundamentales que hace el juez Constitucional, para cada caso en concreto, busca equilibrar la mayor protección de un derecho frente al otro. Por tanto, el art. 15 contentivo del derecho a la protección del dato personal y art. 29 del derecho al debido proceso y prueba legal, deben interpretarse de la mano a derechos sustanciales que regulan actos con efectos jurídicos como lo es la etapa de recolección rastros informáticos por medio de protocolos forenses que arrojan la Evidencia Digital, momento en el cual, la ponderación al derecho a la prueba y el debido proceso serían constitutivos de causal justificante para que sobrevenga un eximente de responsabilidad frente a la protección al dato personal por constituir, una necesidad de probar la comisión de un delito, situación que tanto el responsable y/o Encargante se encuentran obligados para facilitar la actividad investigativa del Estado, su negativa, por el contrario

sería constitutiva de obstaculización a la investigación del estado y no una evidencia de protección al dato personal.

El ciudadano está impedido de evitar la extracción de una Evidencia Digital alegando protección del dato personal cuando su realización viene originaria de una norma imperativa como es el código de procedimiento penal. Por el contrario, cuando la extracción de una evidencia digital depende de la ejecución de una conducta amparada por una norma autorreguladora, ésta facultad la extracción de la evidencia será por una necesidad de obtener la fuente prueba que en la investigación permitirá lleva al convencimiento al juez sobre los hechos delictivos investigados o por el contrario cuando la extracción hace parte del protocolo en atención a incidentes informático, sean o no de índole delictual.

La extracción de la evidencia digital y la protección de datos personales convergen en un punto cuando por un lado será la fuente objeto de la extracción por contener la información y datos, y por otro lado es el dato personal lo que se extrae, por lo tanto es importante que la organización, Estado y persona propietaria de la información y datos, pondere entre su obligación de proteger los datos personales en calidad de responsable y/o encargado del dato y la obligación que tiene frente al Estado para permitir actos de investigación preliminar de un delito o posible delito, en comparación a su facultad autorreguladora para implementar protocolos que permitan generar atención a incidentes vinculando la extracción de evidencia digital sin limitante de la protección de dato personal.

Referencias

Constitución política de 1991.

Colombia. Congreso de la República, Ley 906 de 2004.

Colombia. Congreso de la República, Ley 599 de 2000.

Colombia. Congreso de la República, Ley 1273 de 2009.

Colombia. Congreso de la República, Ley 1266 de 2008.

Colombia. Congreso de la República, Ley 1581 de 2012.

Colombia. Congreso de la República, Decreto 1377 de 2013.

Colombia. Corte Constitucional, Sentencia C-662 de 2000, M.P.: Fabio Morón Díaz.

Colombia. Corte Constitucional, Sentencia C-831 de 2001, M.P.: Álvaro Tafur Galvis.

Colombia. Corte Constitucional, Sentencia C-396 de 2007, M.P.: Marco Gerardo Monroy Cabra.

Colombia. Corte Constitucional, Sentencia C-748 de 2011, M.P.: Jorge Ignacio Pretelt Chaljub.

(DDI), D. D. (2014). OEA. Obtenido de http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_conferencias_varsovia_2013_resol_dirreccion_estrategica.pdf

Black, E. (2001). IBM y El Holocausto. Alemania: Atlántida.

Cano, J. (2010). Computación Forense. Bogotá: Omega.

Cavero, J. M. (1993). El derecho a la Intimidad en la Jurisprudencia Constitucional. Madrid España: Civitas.

Development, O. S. (2014). OSD Global. Obtenido de www.osdglobal.com

Black, E. (2001). *IBM y el Holocausto.* México: Atlántida.

Elneser, A. M. (2013). APROXIMACIÓN A LA INFORMÁTICA FORENSE Y EL DERECHO INFORMÁTICO: Ámbito Colombiano. Medellín: (Departamento Fondo Editorial Funlam) - FUNLAM.

Fiscalía, L. F. (2008). La Prueba en el Proceso Penal Colombiano. Medellín: Fiscalía General de la Nación y Fénix Medina Group.

Peggy Valcke, J. D. (2012). Computer, Law & Security Review – special issue Trust in the Information Society. Oslo, Norway: Editorial Board - University of Oslo.

Sentencia Constitucional, Sentencia T- 419 (Corte Constitucional 8 de julio de 2013).

Sentencia Good Will o Credito Mercantil, expediente 16274 (Consejo de Estado 26 de enero de 2013).

SIC, Delegatura Protección de Datos Personales (2014). Publicación Primera Rendición de Cuentas de Sanciones en 2014. Informe anual. Obtenido de http://www.sic.gov.co/drupal/sites/default/files/files/informe_consolidado_sanciones_1_2014_VERSION_SIC.pdf

Taruffo, M. (2011). *La Prueba de los Hechos* (Cuarta ed.). (J. Feerer, Trad.) Madrid, España: Trotta S.A.

ISO - International Organization for Standarization. (2014). *ISO*. Obtenido de http://www.iso.org/iso/home/about/iso_members.htm?membertype=membertype_MB

ISO BRITANICO. (2014). *Information technology - Security techniques — Incident investigation - principles and processes.* ISO EDITION (UNPUBLISHED)

ICONTEC. (s.f.). *ICONTEC Internacional*. Obtenido de http://icontec.org/index.php/es/portafolio-de-inspeccion/48-colombia/inspeccion/1229-auditoria-interna-iso-17025-y-17020

OCDE. (2002). *organización para la cooperación y desarrollo económico*. Obtenido de http://www.oecd.org/sti/ieconomy/15590267.pdf