

LA INFORMACIÓN RESERVADA EN EL ORDENAMIENTO JURÍDICO COLOMBIANO: REFLEXIONES, PRÁCTICAS E IMPLICACIONES PARA EL DERECHO DISCIPLINARIO

*Julie Paola Camacho Morales**

*Jeimy José Cano Martínez***

*Miguel Gustavo Neira Rueda****

*Vivian Constanza Ovalle Leguizamón*****

*Martha Patricia Villamil Salazar******

* Abogada de la Universidad Industrial de Santander y Especialista en Derecho Administrativo de la Universidad Libre de Colombia. juliepaolacm@gmail.com

** Ingeniero y magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. PhD en Business Administration de Newport University, CA, Estados Unidos. Profesor de cátedra de la Facultad de Derecho de la Universidad de los Andes y de la Facultad de Contaduría de la Universidad Externado de Colombia, en las áreas de derecho informático, evidencia digital, delitos informáticos y seguridad de la información. jjcano@yahoo.com

*** Abogado de la Universidad Católica de Colombia y especialista en Derecho Administrativo de la Universidad Santo Tomás de Aquino de Bucaramanga y en Derecho Comercial de la Universidad Autónoma de Bucaramanga. miguneru05@hotmail.com

**** Abogada de la Universidad Pedagógica y Tecnológica de Colombia. viviabog@gmail.com

***** Abogada de la Universidad Externado de Colombia y magíster en Derecho Penal y Ciencias Criminológicas de la Universidad Externado de Colombia. mapavisa@hotmail.com

Fecha de recepción: 7 de diciembre de 2012. Fecha de modificación: 2 de mayo de 2013. Fecha de aceptación: 5 de julio de 2013. Para citar el artículo: J. PAOLA CAMACHO MORALES, J. JOSÉ CANO MARTÍNEZ *et al.* “La información reservada en el ordenamiento jurídico colombiano: reflexiones, prácticas e implicaciones para el derecho disciplinario”, *Revista Derecho Penal y Criminología*, vol. 34, No. 96, enero-junio 2013, Bogotá, Universidad Externado de Colombia, 2013, pp. 145-185.

Resumen: en el contexto de una sociedad de la información y el conocimiento, en el ejercicio de la función pública se convierte en un reto permanente el adecuado tratamiento de la información, particularmente aquella calificada y establecida por la Constitución y la ley como reservada. Si bien en las iniciativas internacionales de acceso a la información pública se encuentran marcos de referencia asociados con la información reservada, luego de una revisión profunda del marco normativo y jurisprudencial colombiano, se encuentra que no existe una vista homogénea del tema. Esto permite plantear lineamientos y prácticas de seguridad y control que aseguren el cumplimiento del deber funcional de protección de dicha información con arreglo a la ley y teniendo claridad de las responsabilidades y sanciones disciplinarias propias de la relación especial de sujeción de los servidores públicos y particulares que cumplen función pública. **Palabras clave:** información reservada, clasificación de información, prácticas de seguridad y control, acceso a la información pública, sanciones disciplinarias, derecho a la información, tensión entre compartir o proteger, función pública.

RESERVED INFORMATION IN THE COLOMBIAN LAW. CONSIDERATIONS, PRACTICES AND IMPLICATIONS FOR THE DISCIPLINARY LAW

Abstract: In the context of an information society and knowledge, the exercise of public function becomes a permanent challenge to the proper handling of information, particularly the qualified and reserved by the constitution and the law. While international efforts to access to public information frameworks are associated with reserved information, after a thorough review of the legal framework and the Colombian jurisprudential issues, the study finds that there is no a unique view on the subject. This allowed us to propose guidelines and practices in security and control to ensure compliance with the functional duty of protecting such information in accordance with the law, and to have a clear view of the responsibilities and disciplinary sanctions based on special holding relationship by public servants and private employees fulfilling public function. **Keywords:** Reserved information, information classification, security and control practices, access to public information, disciplinary sanctions, right to information, tension between sharing or protect, public function.

INTRODUCCIÓN

Existe una tensión inherente en seguridad de la información que a diario enfrenta la necesidad de compartir información, con sus requerimientos de protección. Si bien cada persona está “facultada” para tener acceso a la información, no toda información está “autorizada” para que sea de dominio público.

Es claro que con la dinámica de la sociedad actual, la privacidad se erosiona cada vez más, esa expresión natural y constitucional que tienen los ciudadanos de mantener en su intimidad aspectos propios de la vida, la cual en sí misma define lo que las personas son y esperan. En este sentido, permanece la clara tendencia de mantener cierto tipo de información en reserva, protegida de “miradas” no autorizadas o de personas que la buscan con intereses diferentes a los que dan lugar a su creación.

Comoquiera que la información, al igual que la energía, no se crea ni se destruye, simplemente se transforma, se hace necesario comprender la esencia de lo que es la información reservada, para establecer prácticas básicas de seguridad y control, que sin menoscabar las garantías propias del “acceso a la información”, pueda accederse a esta en las condiciones requeridas y basada en la valoración de riesgo estimado.

En este sentido, moverse hacia una dinámica de protección de información, como estrategia para acceder de manera confiable a lo que se necesita, exige una disciplina de aseguramiento y entendimiento de la información como activo estratégico de las personas y organizaciones, esto es, una cultura de seguridad de la información que, desde lo que “las personas creen”, posibilite transformar las cosas que se hacen y materializar, con actos visibles y comportamientos confiables, la esencia de la dinámica personal y empresarial: proteger el valor propio y asegurar la construcción de un futuro sostenible¹.

Como consecuencia de lo anterior, la información se convierte en ese elemento fundamental de la vida humana y exigencia natural de la competencia social, empresarial y gubernamental, que alcanza todos los aspectos de la dinámica social, para sumergirnos en una realidad emergente que traspasa nuestros deseos más profundos y descubre las motivaciones más elevadas. La información es la nueva forma de combustible que el mundo necesita y exige para movilizar la energía que transforme personas, sociedades y naciones.

Así pues, el balancear la necesidad de conocer o estar informado, y la reserva o restricción de acceso requerida, es un ejercicio de reconocimiento de los impactos y consecuencias de la revelación de información clasificada, de las bondades de los modelos abiertos y de participación ciudadana, así como de los comportamientos y fines que tanto personas como Estados persiguen, los cuales generalmente se encuentran vinculados con un adecuado tratamiento de la información.

En síntesis, este documento plantea algunas reflexiones que permiten profundizar en las tensiones propias entre el compartir y el proteger, entre el restringir y el revelar, y adelanta una revisión de iniciativas nacionales e internacionales relacionadas con acceso a la información pública como mecanismos de transparencia de las naciones, pasando por un análisis jurisprudencial centrado en el concepto de información reservada, para

1 BROTBY, K. *Information security governance*, cap. 1, John Wiley and Sons, 2009.

establecer elementos conceptuales e implicaciones asociadas con el tratamiento de este tipo de información, así como las conductas relevantes para el derecho disciplinario al respecto. Finalmente, se establece un conjunto base de prácticas y criterios generales que permitan a los servidores públicos o a los particulares que ejercen función pública dar un adecuado tratamiento a la información reservada.

PROTEGER O COMPARTIR: ¿HE AHÍ EL DILEMA!

Con frecuencia se anota que la vida se hace más libre y plena cuando se comparte, cuando se nutre de las realidades de los otros y capitalizamos las lecciones aprendidas que nos permiten ver “por fuera de la caja”. Compartir es un ejercicio de generosidad interior que se traduce en una afinidad trascendente que encuentra en el otro, su mejor destinatario y mejor excusa para construir. Cuando se comparte, las personas experimentan la plenitud de donarse a sí mismas, como esa ofrenda personal que hace, de aquello que se entrega, una expresión íntima de su querer y propio ser.

Compartir en la vida cotidiana, teniendo en cuenta la volubilidad de los seres humanos, previene al hombre sobre sus impactos y riesgos, sobre la forma como será utilizada y, lo que es más importante, sobre la manera como esta podrá ser “manejada” para producir y recrear los intereses de terceros, incluso por encima de los propios. Bien se anota en la literatura especializada que una cosa es nuestra huella digital y otra nuestra sombra digital en internet; la primera se traduce en los rastros que dejamos al navegar por los sitios web alojados en los servidores de la red, y la otra, lo que la información allí publicada dice o revela sobre nosotros².

En este contexto, la información que se maneja a diario requiere ser analizada frente a los riesgos propios de su tratamiento, para evitar que “terceros” sin autorización, o personas con intenciones desconocidas, puedan invadir los terrenos de la esfera personalísima y poner en peligro su integridad en un contexto de cambios y dinámica internacional.

Con esto no se quiere indicar que exista una motivación extraña o deseos ocultos de personas u organizaciones frente a la información personal, estatal o empresarial, que genere “delirios” de persecución y permanente zozobra e inquietud en las organizaciones e individuos, sino más bien plantear una reflexión propositiva que permita ubicar a la información como ese elemento estratégico que hace la diferencia en el mundo personal, estatal y empresarial.

2 GANTZ *et al.* The diverse and exploding digital universe. *IDC Research*, 2008. Disponible en: www.emc.com/collateral/analyst-reports/diverse-exploding-digital-universe.pdf (consultado: 21-05-2012).

De acuerdo con FOSTER³, existe un espectro de análisis entre el compartir y el proteger que permite entender mejor las tensiones propias de estas dos distinciones, esto en el ámbito empresarial. Para ello define ocho variables complementarias entre sí que revelan motivaciones y declaraciones que son claves para avanzar en el estudio del balance requerido de las dos vistas sobre la información; aquellas son: las leyes, lo requerido por la industria, la necesidad de minimizar pérdidas, la revelación de vulnerabilidades, las expectativas públicas, el valor financiero, la reputación y la recomendación de la industria.

Cuando el movilizador del tema son las *regulaciones o leyes*, comenta FOSTER, se establece que “la información es protegida internamente pues existen normas o estatutos que dictan un mandato sobre el aseguramiento de su confidencialidad”, cuyo incumplimiento genera impactos negativos, bien de carácter sancionatorio interno con repercusiones externas, o exclusiones definitivas en ciertos sectores de negocio.

Del mismo modo, cuando el tema se apalanca en aquello *requerido por la industria*, “la información se protege dado que es una práctica estándar en la industria, lo cual implica habilidades de aseguramiento”. Esto significa que, para un sector particular, son criterios de ingreso y aceptación, la acreditación de prácticas en tratamiento de la información como base de la relación de confianza entre sus miembros.

Así mismo, si lo que moviliza el adecuado tratamiento de la información es *minimizar las pérdidas*, la declaración se articula como “la información se protege limitando el acceso de las personas a la misma, para prevenir su pérdida hacia el exterior”. Esta declaración busca asegurar las responsabilidades de los participantes frente a la información y prevenir fugas o pérdidas de información intencionales y no intencionales.

De otra parte, cuando hablamos de *revelación de vulnerabilidad*, FOSTER expresa: “la información se protege, pues es viable descubrir fallas que pueden ser explotadas por terceros y alcanzar elementos valiosos de la empresa o la información”. Esta expresión nos muestra la sensibilidad del manejo de las debilidades de seguridad y control, las cuales, si no observan un tratamiento adecuado, pueden causar detrimento o compromiso del nivel de confianza en sus grupos de interés.

Si el movilizador son las *expectativas públicas*, el tratamiento de la información estará articulado con la confianza que los terceros tienen del aseguramiento de la confidencialidad de su información frente al acceso por parte de una organización o personas autorizadas. La confianza es el valor fundamental sobre el cual descansa la promesa empresarial del acceso a la información personal y corporativa, una forma para construir en conjunto distintos futuros posibles⁴.

3 FOSTER, C. Sharing o controlling? Examining the decision to segregate information within the organization. *ISACA Journal*, vol. 2, 2012.

4 HAMEL, G. *Lo que importa ahora. Cómo triunfar en un mundo de cambios implacables, competencia feroz e innovación sin barreras*, sección 3.5, Norma, 2012.

Por otro lado, si la información requiere ser protegida por *el valor que representa*, esto es, que puede ser aprovechada para alcanzar ganancias económicas, estamos hablando de la protección del conocimiento inherente a la información y lo que ello significa en términos financieros. Es decir, cómo las empresas aseguran aquellos elementos sensibles que marcan la diferencia en su sector y generan diferenciación del valor frente a sus competidores⁵.

No hay duda que *la reputación* es un factor clave que protege el adecuado tratamiento de la información. En este sentido, la información revestida de su valor estratégico debe ser asegurada para minimizar los impactos de una eventual fuga de información, que afecte su imagen, genere sanciones legales, pérdidas de clientes o posición privilegiada en su ámbito de negocio.

Finalmente, y no menos importante, la información debe ser protegida atendiendo las *recomendaciones que la industria establece* para mantener un nivel de aseguramiento que permita una relación homogénea para sintonizar los deseos de compartir y la necesidad de proteger aquello que se declara valioso para ambas partes. Las prácticas definidas por la industria establecen la base homogénea para comprender los riesgos propios del tratamiento de la información.

En conclusión, es posible afirmar que cualquiera de estas variables establece una forma concreta de elevar la discusión de la protección de la información, del ámbito puramente técnico de operación, a los impactos y efectos, que bien marcan las consecuencias a las cuales eventualmente la organización estará expuesta y la forma de llamar la atención y hacer parte de la agenda de alta gerencia.

Este tema, aplicado al Estado y a la sociedad en general, permite visualizar con las mismas perspectivas los riesgos de la difusión no controlada de información que deba estar sometida a reserva y la necesidad de medios y métodos para protegerla, ello respecto a los fines del Estado y los derechos fundamentales de las personas.

LA INFORMACIÓN RESERVADA EN LA NORMATIVIDAD Y JURISPRUDENCIA COLOMBIANA

Considerando lo dispuesto en el artículo 74 de la Constitución Política de 1991⁶, el acceso a la información debe ser entendido como un derecho y, en razón a ello, solamente puede ser limitado por disposición constitucional o legal expresa.

5 HAX, A. *El modelo delta. Un nuevo marco estratégico*, 2003. Disponible en: <http://cirpq.tripod.com/consultoriaestrategica/modelodelta.pdf> (consultado: 21-05-2012).

6 “Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley”.

En desarrollo de este precepto constitucional, en el Congreso de la República recientemente se tramitó el Proyecto de Ley 156 de 2011 Senado, 226 de 2011 Cámara, por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones⁷; en el artículo 2.º del texto conciliado se propuso como principio lo siguiente:

Artículo 2º. Principio de máxima publicidad para titular universal. Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la presente ley⁸.

De igual manera, en el mismo proyecto de ley, el cual está *ad portas* de convertirse en ley de la República, se establecen otros principios que rigen el acceso a la información, como los siguientes: transparencia, buena fe, facilitación, no discriminación, gratuidad, celeridad, eficacia, calidad de la información, divulgación proactiva de la información y responsabilidad del uso de la información.

Esta condición de que el acceso a la información sea restringido exclusivamente por la Constitución o la Ley, se debe a que dicho acceso es considerado como un derecho que ostenta todo ciudadano; en este sentido, en providencia de la Corte Constitucional, T-158 del 24 de marzo de 1994, con ponencia del honorable magistrado HERNANDO HERRERA VERGARA, se expuso que este derecho tiene carácter específico y autónomo; de igual manera, en pronunciamiento anterior de la misma Corporación del año 1992, se definió de la siguiente manera:

El derecho a la información no es solamente el derecho a informar, sino también el derecho a estar informado. El artículo 74 de la Constitución Nacional, al consagrar el derecho de acceder a los documentos públicos, hace posible el ejercicio del derecho a la información, y de esta manera los demás derechos fundamentales ligados al mismo. El acceso a los documentos públicos no se traduce necesariamente en una petición o en la adquisición de nueva información. Es, pues, independiente tanto de la petición como de la información y, como tal, plenamente autónomo y con universo propio.

7 De acuerdo con el *Diario Oficial* n.º 417 del 10 de julio de 2012, el 19 de junio de 2012 se presentó en el Congreso de la República el informe del proyecto de conciliación del Proyecto de Ley 156 de 2011 Senado, 226 de 2011 Cámara, por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones; una vez aprobado dicho texto conciliado, se remitió al presidente de la República el citado proyecto de ley para su sanción, y el cual a agosto de 2012 no ha sido promulgado; en consecuencia este proyecto de ley aún continúa para sanción presidencial.

8 *Diario Oficial* n.º 417 del 10 de julio de 2012, proyecto de ley número 156 de 2011 Senado, 226 de 2011 Cámara, por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones, p. 45.

(...) es cierto que el derecho a acceder a los documentos públicos consagrado en el artículo 74, puede considerarse en buena medida como una modalidad del derecho fundamental de petición y como instrumento necesario para el ejercicio del derecho a la información y, por lo tanto, comparte con estos su núcleo axiológico esencial, no lo es menos que tiene también un contenido y alcance particulares que le otorgan especificidad y autonomía dentro del conjunto de los derechos fundamentales.

En efecto, es claro que dentro de las facultades del titular de este derecho se encuentra la de hacer una simple consulta de los documentos que no culmine, si así lo estima conveniente, en la formulación de petición alguna. Como también la consulta de documentos con la específica finalidad no ya de adquirir información adicional, sino de aclarar o constatar la ocurrencia de una típica práctica o conducta de desinformación⁹.

En el mismo sentido de definir el acceso a la información como un derecho, la Corte, en la sentencia C-488 de 1993, definió la noción de lo que es el derecho a la información diciendo que es “un derecho que expresa la tendencia natural del hombre hacia el conocimiento. El ser humano está abierto a la aprehensión conceptual del entorno para reflexionar y hacer juicios y raciocinios sobre la realidad. Es en virtud de esta tendencia que a toda persona se le debe la información de la verdad, como exigencia de su ser personal”¹⁰.

Posteriormente la misma Corte Constitucional, exponiendo otra tesis sobre el concepto de que el acceso a la información debe ser entendido como un derecho especial y autónomo, expresó:

En principio, la Constitución no consagra un derecho general a la información exigible por toda persona de las autoridades y los particulares. La ley establece los casos en que las autoridades y los particulares están obligados a informar de las actuaciones o de lo relativo a una relación o negocio jurídico. No obstante, un deber excepcional de información se deduce de los principios de solidaridad (CP art. 1) y de eficacia de los principios, derechos y deberes (CP art. 2), en casos en que la existencia autónoma y libre de una persona dependa del suministro de la información y su omisión vulnera directamente un derecho fundamental, sin que sean suficientes los remedios legales para impedirlo¹¹.

9 Corte Constitucional. Sentencia T-473 del 14 de julio de 1992. Sala de Revisión número 1. Tutela número 1815. M.P.: CIRO ANGARITA BARÓN.

10 Corte Constitucional. Sentencia C-488 del 28 de octubre de 1993. Expediente D-272. M.P.: VLADIMIRO NARANJO MESA.

11 *Ibíd.* Sentencia T-443 del 12 de octubre de 1994.

Continuando con la determinación del acceso a la información como un derecho, en jurisprudencia constitucional se le otorgó a este derecho la característica especial de ser un derecho de doble vía; concretamente en sentencia T-332 de 1993, con ponencia del magistrado JOSÉ GREGORIO HERNÁNDEZ GALINDO, se expresó:

Recuérdese, sin embargo, que el derecho a la información es de doble vía, característica trascendental cuando se trata de definir su exacto alcance: no cobija únicamente a quien informa (sujeto activo) sino que cubre también a los receptores del mensaje informativo (sujetos pasivos), quienes pueden y deben reclamar de aquel, con fundamento en la misma garantía constitucional, una cierta calidad de la información. Esta debe ser, siguiendo el mandato de la misma norma que reconoce el derecho, “veraz e imparcial”. Significa ello que no se tiene simplemente un derecho a informar, pues el Constituyente ha calificado ese derecho definiendo cuál es el tipo de información que protege. Vale decir, la que se suministra desbordando los enunciados límites –que son implícitos y esenciales al derecho garantizado– realiza anti-valores (falsedad, parcialidad) y, por ende, no goza de protección jurídica; al contrario, tiene que ser sancionada y rechazada porque así lo impone un recto entendimiento de la preceptiva constitucional¹².

Como se expresa en la jurisprudencia constitucional que ha precisado la naturaleza, el contenido y los alcances del derecho de acceso a la información, se ha destacado la relación entre este derecho y el funcionamiento del modelo democrático, pues de esta manera se permite la materialización de los principios de transparencia y publicidad que deben regir el actuar de la administración pública¹³; al respecto esta Corporación en sentencia T-1025 de 2007 sostuvo: “(...) la importancia del derecho a acceder a la información para garantizar la transparencia y la publicidad de la gestión pública, condiciones fundamentales para impedir la arbitrariedad estatal y para asegurar la vigencia de un Estado democrático y respetuoso de los derechos fundamentales de las personas”¹⁴.

Zanjando toda duda con relación a la consideración de si el acceso a la información es o no un derecho, el proyecto de ley precitado, que se encuentra para sanción presidencial, en el artículo 4 definió el derecho al acceso a la información de la siguiente manera:

Artículo 4°. Concepto del derecho. En ejercicio del derecho fundamental de acceso a la información, toda persona puede conocer sobre la existencia y acceder

12 Corte Constitucional. Sentencia T-332 del 12 de agosto de 1993. Sala Quinta de Revisión. Expediente T-12350. Magistrado ponente: JOSÉ GREGORIO HERNÁNDEZ GALINDO.

13 Corte Constitucional. Sentencia T-161 del 10 de marzo de 2011. Expediente T-2843676. M.P.: HUMBERTO ANTONIO SIERRA PORTO.

14 Corte Constitucional. Sentencia T-1025 del 3 de diciembre de 2007. Expediente T-1401460. M.P.: MANUEL JOSÉ CEPEDA ESPINOSA.

a la información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente. Las excepciones serán limitadas y proporcionales, deberán estar contempladas en la ley o en la Constitución y ser acordes con los principios de una sociedad democrática.

El derecho de acceso a la información genera la obligación correlativa de divulgar proactivamente la información pública y responder de buena fe, de manera adecuada, veraz, oportuna y accesible a las solicitudes de acceso, lo que a su vez conlleva la obligación de producir o capturar la información pública. Para cumplir lo anterior los sujetos obligados deberán implementar procedimientos archivísticos que garanticen la disponibilidad en el tiempo de documentos electrónicos auténticos¹⁵.

A su vez, la Corte Constitucional, en pronunciamiento del 27 de junio de 2007, realizó un estudio exhaustivo del derecho a la información en el derecho constitucional, y del cual concluyó:

Las disposiciones y la doctrina nacional sobre límites del derecho de acceso a la información pública se encuentran en estrecha relación con las disposiciones y la doctrina internacional en la materia. Como lo indica el Procurador General, distintos órganos de supervisión de tratados internacionales han llegado a conclusiones similares a las que se han presentado en los fundamentos anteriores. En este sentido, no sobra recordar que a la luz de lo dispuesto en el artículo 93 de la Constitución, los tratados y convenios internacionales ratificados por Colombia y la doctrina de los órganos autorizados para su protección constituyen criterios relevantes de interpretación del alcance de los derechos constitucionales fundamentales. En tal virtud, la norma legal demandada debe ser estudiada no solo a la luz de la doctrina constitucional interna sobre el derecho de acceso a la información, sino teniendo seriamente en cuenta lo prescrito por el artículo 13 de la Convención Americana sobre Derechos Humanos, el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos y la doctrina de los órganos autorizados para su interpretación y defensa. Pasa la Corte a hacer un breve resumen de la doctrina internacional más relevante a la hora de resolver el problema jurídico planteado¹⁶.

15 *Diario Oficial* n.º 417 del 10 de julio de 2012, Proyecto de Ley 156 de 2011 Senado, 226 de 2011 Cámara, por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones, p. 46.

16 Corte Constitucional. Sentencia C-491 del 27 de junio de 2007. Expediente D-6583. M.P.: JAIME CÓRDOBA TRIVIÑO.

De esta forma, revisada la jurisprudencia citada, se obtiene que el acceso a la información es un derecho de carácter especial, autónomo, de doble vía, que prevalece en una eventual colisión de derechos y que se deriva de lo dispuesto en los artículos 1, 2 y 74 de la Constitución Política de Colombia, pero, como se ha afirmado anteriormente, este derecho puede ser limitado exclusivamente por la misma Constitución o la ley; esta posibilidad jurídica de limitar el acceso, en la providencia del año 1992 ya mencionada, se justificó trayendo a colación lo expuesto en la asamblea constituyente, de la siguiente manera:

En las labores preparatorias de la Asamblea Nacional Constituyente se manifestó claramente la idea de que la información pertenece al público pero que no todo lo que es técnicamente informable es ético y jurídicamente informable. Se pone así de presente la responsabilidad de los medios en la producción de sus mensajes, en la prevención de la anarquía y en la práctica de la tolerancia. Todo lo cual supone un permanente sentido de responsabilidad y objetividad en la presentación de la información¹⁷.

Con este mismo lineamiento jurisprudencial, en sentencia T-066 del 5 de marzo de 1998 se justificó la limitación al acceso a la información de la siguiente manera:

Con todo, el mismo artículo 74 de la Constitución autoriza a la ley para determinar que el público no tenga acceso a ciertos documentos oficiales. Asimismo, la sentencia transcrita parcialmente admite la consagración de excepciones a la regla de la publicidad, al expresar que “la publicidad como principio constitucional que informa el ejercicio del poder público se respeta cuando se logra mantener como regla general y siempre que la excepción, contenida en la ley, sea razonable y ajustada a un fin constitucionalmente admisible”.

De lo anterior se concluye que también en los Estados democrático-liberales pueden existir informaciones de carácter reservado, es decir, que no deben ser conocidas por el público. De manera general, será la ley la que establezca cuáles informaciones deberán tener esa calidad. Las restricciones que surjan de esa ley podrán ser sometidas a examen de constitucionalidad, fundamentalmente para establecer si no vulneran el principio de proporcionalidad y si resultan compatibles con una sociedad democrática avanzada¹⁸.

17 Subcomisión 0403: *Libertad de información y medios de comunicación*, informe final. En: Presidencia de la República, *Propuestas de las comisiones preparatorias*, Bogotá, enero de 1991, pp. 214-216. Citado en Corte Constitucional, sentencia T-473 del 14 de julio de 92. Sala de Revisión número 1. Tutela número 1815. M.P.: CIRO ANGARITA BARÓN.

18 Corte Constitucional. Sentencia T-066 del 5 de marzo de 1998. Expediente T-145002. M.P.: EDUARDO CIFUENTES MUÑOZ.

Al revisar la constitucionalidad de las normas que declaran cierta información como reservada, la Corte ha aplicado el criterio de proporcionalidad para establecer la exequibilidad o no de dicha declaración; concretamente en sentencia del 30 de septiembre de 2003, con ponencia de la magistrada CLARA INÉS VARGAS HERNÁNDEZ, se afirmó lo siguiente:

El principio de proporcionalidad se asienta sobre dos supuestos concretos: uno formal, constituido por el principio de legalidad, y otro material, conocido como principio de justificación teleológica.

El primero exige que toda medida limitativa de un derecho fundamental, en este caso el acceso a documentos públicos, se encuentre prevista en la ley. Se considera un presupuesto formal ya que no asegura un contenido determinado de la medida, pero sí constituye un postulado básico para su legitimidad democrática y asegura la previsibilidad de la actuación de los poderes públicos.

El segundo presupuesto es de orden material porque introduce en el enjuiciamiento de las intromisiones del Estado en la esfera de los derechos fundamentales los valores que trata de salvaguardar la actuación de los poderes públicos y que precisan gozar de la fuerza constitucional suficiente para enfrentarse a los valores representados por los derechos fundamentales restringidos. Así pues, el principio de proporcionalidad requiere que toda limitación a los derechos fundamentales tienda a la consecución de fines legítimos^{19,20}.

Finalmente, en la sentencia C-872 de 2003, sobre este mismo tema dijo la Corporación:

(L)as excepciones al acceso a la información solamente se admiten si tienen por objetivo proteger un derecho fundamental o algún bien de especial importancia, como lo es la seguridad nacional. Para tal efecto se debe acreditar que tales derechos o bienes se verían seriamente afectados si se difunde determinada información, lo que hace necesario mantener la reserva²¹.

En concordancia con todo lo anterior, se tiene que es válido limitar el derecho al acceso a la información, pero esta facultad delegada en cabeza del legislador no es absoluta; con este derrotero, en sentencia del 24 de septiembre de 2004 se expuso:

En otras palabras, la confidencialidad de los documentos públicos en un Estado Democrático no puede ser absoluta, comoquiera que la regla general es

19 GONZÁLEZ-CUÉLLAR SERRANO, NICOLÁS. *Proporcionalidad y derechos fundamentales en el proceso penal*, Madrid, 1995.

20 Sentencia C-872 del 30 de septiembre 2003. Expediente D-4537. M.P.: CLARA INÉS VARGAS HERNÁNDEZ.

21 Corte Constitucional. Sentencia C-872 del 30 de septiembre de 2003. Expediente D-4537. M.P.: CLARA INÉS VARGAS HERNÁNDEZ.

el principio de publicidad en la actuación de las autoridades y la excepción es la reserva; por consiguiente, el operador jurídico no solo debe valorar que una norma de rango legal autorice la reserva del documento, sino cuáles derechos, principios y valores constitucionales están afectados con la restricción, ya que en algunas ocasiones deberán prevalecer los derechos, valores y principios que inspiran la confidencialidad de la información, y en otros, los que se le oponen. Así las cosas, ponderados los intereses en juego, puede que la reserva de un documento prevalezca ante derechos como a la información; pero debe ceder frente a otros como los derechos a la defensa y de acceso a la administración de justicia, los cuales, *prima facie*, tienen mayor importancia en las sociedades democráticas modernas²².

En resumen, en sentencia C-491 del 27 de junio de 2007, la cual es reiterada en pronunciamientos posteriores, la Corte ha considerado que solo es legítima una restricción del derecho de acceso a la información pública o el establecimiento de una reserva legal sobre cierta información cuando:

- i) la restricción está autorizada por la ley o la Constitución;
- ii) la norma que establece el límite es precisa y clara en sus términos de forma tal que no ampare actuaciones arbitrarias o desproporcionadas de los servidores públicos;
- iii) el servidor público que decide ampararse en la reserva para no suministrar una información motiva por escrito su decisión y la funda en la norma legal o constitucional que lo autoriza;
- iv) la ley establece un límite temporal a la reserva;
- v) existen sistemas adecuados de custodia de la información;
- vi) existen controles administrativos y judiciales de las actuaciones o decisiones reservadas;
- vii) la reserva opera respecto del contenido de un documento público pero no respecto de su existencia;
- viii) la reserva obliga a los servidores públicos comprometidos pero no impide que los periodistas que acceden a dicha información puedan publicarla;

22 Corte Constitucional. Sentencia T-928 del 24 de septiembre de 2004. Expediente T-928730. M.P.: JAIME ARAÚJO RENTERÍA.

ix) la reserva se sujeta estrictamente a los principios de razonabilidad y proporcionalidad;

x) existen recursos o acciones judiciales para impugnar la decisión de mantener en reserva una determinada información²³.

En la misma sentencia, una vez realizado un minucioso estudio de derecho normativo internacional, el cual es válido a partir de la aplicación del bloque de constitucionalidad instituido en el artículo 93 de la Constitución Política de 1991, la Corte en ese momento concluyó:

En suma, el derecho internacional protege expresamente el derecho de acceso a la información pública y establece rigurosos requisitos para admitir una restricción a tal derecho. i) En primer lugar cualquier restricción tiene que encontrarse amparada expresamente en una norma legal o constitucional. ii) En segundo lugar, la restricción debe ser temporal. iii) En tercer lugar la restricción debe resultar necesaria para asegurar los bienes y derechos propios de una sociedad democrática. iv) Los criterios de reserva de información deben ser establecidos en forma clara y precisa para permitir que entes jurídicos puedan revisar tanto la legalidad como la razonabilidad de la resolución a la luz de los intereses afectados. v) El funcionario público que aplica la reserva está obligado a motivar su decisión en dichos criterios. v) Finalmente, toda norma o decisión administrativa en esta materia debe ser susceptible de ser controlada por un funcionario judicial objetivo, independiente e imparcial que pueda valorar la proporcionalidad y razonabilidad de la limitación.

Adicionalmente, las normas de derecho internacional admiten que pueda existir una reserva con la finalidad de garantizar la defensa y seguridad nacional. Sin embargo, señalan que en todo caso es necesario satisfacer los requisitos antes mencionados, en particular, los principios de razonabilidad y proporcionalidad de la restricción. En otras palabras, indican que para limitar un derecho de la importancia del derecho de acceso a la información pública no basta con apelar a conceptos amplios y de notable nivel de abstracción como el concepto de defensa y seguridad nacional²⁴.

Ahora bien, ese derecho al acceso a la información, a la libertad de pensamiento y expresión²⁵ tiene límites, como se ha visto, que son principalmente el derecho a la in-

23 Corte Constitucional. Sentencia C-491 del 27 de junio de 2007. Expediente D-6583. M.P.: JAIME CÓRDOBA TRIVIÑO.

24 Corte Constitucional. Sentencia C-491 del 27 de junio de 2007. Expediente D-6583. M.P.: JAIME CÓRDOBA TRIVIÑO.

25 Convención Americana sobre Derechos Humanos. Artículo 13: "(1). Toda persona tiene derecho a la

timidad y el buen nombre²⁶ y a la honra²⁷ de todas las personas, derechos protegidos y consagrados en la Constitución Política de Colombia y en los diferentes instrumentos de Derecho Internacional, como las Declaraciones de Derechos Humanos, Tratados y Convenciones, así como otros límites trazados por la seguridad nacional y la prevalencia del interés general²⁸; es deber de los servidores públicos cumplir con los fines del Estado, en particular la defensa de los derechos de las personas que residen en el territorio nacional, de modo que la tensión existente entre el compartir y el proteger también involucra estos aspectos que finalmente resultan relevantes para el derecho disciplinario, como se verá más adelante.

libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. (2) El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar: (a) el respeto a los derechos o a la reputación de los demás, o (b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas. (3) No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones. (4) Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2. (5) Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional”.

- 26 Constitución Política de Colombia. Artículo 25: “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Solo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley”.

- 27 Constitución Política de Colombia. Artículo 21: “Se garantiza el derecho a la honra. La ley señalará la forma de su protección”.
- 28 Constitución Política de Colombia. Artículo 2: “Son fines esenciales del Estado: servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo. Las autoridades de la república están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias y demás derechos y libertades, y asegurar el cumplimiento de los deberes sociales del Estado y de los particulares”.

LA CLASIFICACIÓN DE LA INFORMACIÓN EN EL CONTEXTO JURÍDICO COLOMBIANO

Establecido hasta este punto el marco jurídico conceptual en el que se encuentra desarrollado el concepto de información reservada, es pertinente de acuerdo con lo propuesto en la parte introductoria de este artículo y teniendo presente la tensión inherente entre el compartir y proteger, pasar a establecer los criterios de clasificación de la información y de esta manera determinar la noción de información reservada.

En cuanto a la clasificación de la información a partir de la normatividad y la jurisprudencia, se establecerán las definiciones que se han emitido acerca de conceptos relevantes para este estudio, tales como: información, información pública, información privada, información semiprivada e información restringida.

De esta manera, manteniendo la actualidad del presente escrito es necesario iniciar refiriéndose a las definiciones contenidas en el proyecto de ley por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional, proyecto el cual, como se mencionó anteriormente, se encuentra para sanción presidencial y que una vez vencido el término para objetar por parte del presidente de la República, de acuerdo con la normas procedimentales, este está obligado en la actualidad a sancionarla y de esta manera emitirla como ley de la República; de ahí la necesidad y pertinencia de tener en cuenta lo preceptuado en dicho proyecto legislativo.

Artículo 6°. Definiciones.

a) Información. Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

b) Información pública. Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

c) Información pública clasificada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley.

d) Información pública reservada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.

De esta transcripción se resalta que en cuanto al concepto base de este escrito, “información reservada”, se le agrega el calificativo de público; esto en razón a que el proyecto de ley analizado está dirigido a las entidades públicas o particulares que desempeñen funciones públicas; en consecuencia, lo que se define es la información emitida por esta clase de entes²⁹.

Identificando en la normatividad otros conceptos relevantes, en la Ley Estatutaria 1266 del 31 de diciembre de 2008, mediante la cual se dictan las disposiciones generales del *habeas data* y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones³⁰, se establecieron las siguientes definiciones adicionales:

Artículo 3o. Definiciones. Para los efectos de la presente ley, se entiende por:

a) Titular de la información. Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de *habeas data* y demás derechos y garantías a que se refiere la presente ley;

b) Fuente de información. Es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y respon-

29 Concretamente, de acuerdo con el artículo 5 del mismo proyecto se establece que el ámbito de aplicación va dirigido a: a) Toda entidad pública, incluyendo las pertenecientes a todas las Ramas del Poder Público, en todos los niveles de la estructura estatal, central o descentralizada por servicios o territorialmente, en los órdenes nacional, departamental, municipal y distrital; b) Los órganos, organismos y entidades estatales independientes o autónomos y de control; c) Las personas naturales y jurídicas, públicas o privadas, que presten función pública, que presten servicios públicos respecto de la información directamente relacionada con la prestación del servicio público; d) Cualquier persona natural, jurídica o dependencia de persona jurídica que desempeñe función pública o de autoridad pública, respecto de la información directamente relacionada con el desempeño de su función; e) Las empresas públicas creadas por ley, las empresas del Estado y sociedades en que este tenga participación; f) Los partidos o movimientos políticos y los grupos significativos de ciudadanos; g) Las entidades que administren instituciones parafiscales, fondos o recursos de naturaleza u origen público. Las personas naturales o jurídicas que reciban o intermedien fondos o beneficios públicos territoriales y nacionales y no cumplan ninguno de los otros requisitos para ser considerados sujetos obligados, solo deberán cumplir con la presente ley respecto de aquella información que se produzca en relación con fondos públicos que reciban o intermedien.

30 Revisada constitucionalmente mediante la sentencia C-1011 del 16 de octubre de 2008, la Corte Constitucional efectuó la revisión de constitucionalidad del Proyecto de Ley Estatutaria No. 27/06 Senado, 221/07 Cámara (Acum. 05/06 Senado).

sabilidades de ambos. La fuente de la información responde por la calidad de los datos suministrados al operador la cual, en cuanto tiene acceso y suministra información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos;

(...)³¹.

Determinadas las definiciones a partir de la normatividad especial existente, en sentencia T-729 del 5 de septiembre de 2002, reiterada en otros pronunciamientos como la sentencia C-336 de 2007, la Corte estableció cuatro grandes tipos de información: la información pública o de dominio público, la información semiprivada, la información privada y la información reservada o secreta; conceptos que definió de la siguiente manera:

[i] *información pública*, calificada como tal según los mandatos de la ley o de la Constitución, puede ser obtenida y ofrecida sin reserva alguna y sin importar si la misma sea información general, privada o personal. Por vía de ejemplo, pueden contarse los actos normativos de carácter general, los documentos públicos en los términos del artículo 74 de la Constitución, y las providencias judiciales debidamente ejecutoriadas; igualmente serán públicos, los datos sobre el estado civil de las personas o sobre la conformación de la familia. Información que puede solicitarse por cualquier persona de manera directa y sin el deber de satisfacer requisito alguno.

La *información semiprivada*, será aquella que por versar sobre información personal o impersonal y no estar comprendida por la regla general anterior, presenta para su acceso y conocimiento un grado mínimo de limitación, de tal forma que la misma solo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Es el caso de los datos relativos a las relaciones con las entidades de la seguridad social o de los datos relativos al comportamiento financiero de las personas.

La *información privada*, será aquella que por versar sobre información personal o no, y que por encontrarse en un ámbito privado, solo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, de los documentos privados, de

31 *Diario Oficial* n.º 47.219 de 31 de diciembre de 2008. Ley Estatutaria 1266 del 31 de diciembre de 2008, mediante la cual se dictan las disposiciones generales del *habeas data* y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

las historias clínicas o de la información extraída a partir de la inspección del domicilio.

La *información reservada*, que por versar igualmente sobre información personal y sobre todo por su estrecha relación con los derechos fundamentales del titular –dignidad, intimidad y libertad– se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones. Cabría mencionar aquí la información genética, y los llamados “datos sensibles” o relacionados con la ideología, la inclinación sexual, los hábitos de la persona, etc.³² (cursivas fuera de texto).

Con lo expuesto hasta este punto, se tiene que la información reservada es la excepción a la regla general de acceso a la información; este último es un derecho, y de acuerdo con los criterios de reserva legal y proporcionalidad, establecidos en la jurisprudencia, se pasa a establecer casos concretos de declaratoria de reserva de la información.

Así las cosas, un concepto es la información sometida a reserva, la cual se encuentra documentada en las diferentes consideraciones legislativas del orden nacional, y otro, la definición de información reservada, que restringe taxativamente su acceso por estar asociada con los datos sensibles, que pueden llevar a discriminación o afectación directa de la dignidad, la libertad y la intimidad.

En este sentido, y revisado el ordenamiento jurídico colombiano, no se encuentra una ley que establezca todos y cada uno de los documentos que tienen el carácter de reservados; en consecuencia, se encuentra a cargo de la entidad consultada o el funcionario público o particular establecer si la información requerida se encuentra provista de reserva; por lo tanto, queriendo realizar un aporte adicional, de manera enunciativa se establecerá la información o documentos que tienen carácter reservado, identificando la disposición normativa que declaró dicha información como tal.

Se determina el listado como enunciativo, ya que debido a lo disperso y extenso de las disposiciones normativas que declaran cierta información como reservada, se hace un trabajo muy dispendioso el establecer todas y cada una de las normas que contienen una declaración de tal índole, pues de lograrlo se realizaría un listado taxativo que a la actualidad en el ordenamiento jurídico colombiano no ha existido.

En consecuencia, teniendo en cuenta la anterior salvedad y queriendo proporcionar una guía enunciativa, se realiza el siguiente listado de declaraciones de reserva de la información:

32 Corte Constitucional. Sentencia T-729 del 5 de septiembre de 2002. Expediente T-467467. M.P.: EDUARDO MONTEALEGRE LYNETT.

1. Las cartas y papeles privados. Según el artículo 15 de la Constitución Política, la correspondencia y demás formas de comunicación privada son inviolables. Solo pueden ser interceptadas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

2. Información que vulnere el derecho a la intimidad (C. N. art. 15).

3. Reserva de información. El Fondo de Garantías estará obligado a guardar reserva sobre las informaciones que exija a las instituciones inscritas, salvo los casos previstos en la Constitución y la ley. En general, el Fondo gozará de reserva sobre sus papeles, libros y correspondencia. (Decreto 663 del 2 de abril de 1993).

4. Los proveedores de redes y servicios de telecomunicaciones, los funcionarios de la Fiscalía General de la Nación y aquellos que ejerzan funciones de Policía Judicial que tengan acceso a cualquier tipo de información o datos con ocasión o en ejercicio de sus funciones o participen en actividades relacionadas con la interceptación de comunicaciones, se obligan a garantizar la reserva de los datos y la confidencialidad de la información, so pena de las investigaciones penales y disciplinarias a que haya lugar. (Decreto 1704 del 15 de agosto de 2012).

5. En la evaluación de la capacidad psicofísica y de la disminución de la capacidad laboral, y aspectos sobre incapacidades, indemnizaciones, pensión por invalidez e informes administrativos por lesiones, de los miembros de la Fuerza Pública, alumnos de las Escuelas de Formación y sus equivalentes en la Policía Nacional, personal civil al servicio del Ministerio de Defensa Nacional y de las Fuerzas Militares y personal no uniformado de la Policía Nacional vinculado con anterioridad a la vigencia de la Ley 100 de 1993. Las causales de no aptitud que resulten de los exámenes practicados en los diferentes eventos del servicio tienen carácter de reservado. En consecuencia, tales causales y la historia clínica no forman parte de los informes que se dirijan a los distintos comandos. (Decreto 1796 del 14 de septiembre de 2000).

6. La Ley 23 de 1981, “por la cual se dictan normas en materia de Ética Médica”, en su artículo 34 define que la historia clínica es un documento privado sometido a reserva, que únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos en la ley.

7. Harán parte de la reserva las investigaciones preliminares, los pliegos y autos de cargos que formulen la Procuraduría General de la Nación y demás órganos de control dentro de los procesos disciplinarios y de responsabilidad fiscal, lo mismo que los respectivos descargos; los fallos serán públicos. La violación de la reserva será causal de mala conducta. (Ley 190 del 6 de junio de 1995).

8. Reserva de la actuación disciplinaria. En el procedimiento ordinario las actuaciones disciplinarias serán reservadas hasta cuando se formule el pliego de cargos o la pro-

videncia que ordene el archivo definitivo, sin perjuicio de los derechos de los sujetos procesales. En el procedimiento especial ante el Procurador General de la Nación y en el procedimiento verbal, hasta la decisión de citar a audiencia. (Art. 95 de la Ley 734 de 2002).

9. La información relacionada con gastos reservados gozará de reserva legal por un término de 20 años, sin perjuicio de las investigaciones de orden penal, disciplinario o fiscal.

Con excepción del control político que determina la Constitución Nacional y de las investigaciones formales de que trata el inciso anterior, la información a que se refiere el presente artículo solo podrá ser examinada por el grupo auditor definido en el artículo 4.º de la presente ley. (Ley 1097 del 2 de noviembre de 2006).

La información por su carácter reservado no podrá hacerse pública y el informe respectivo se rendirá en informe separado que tendrá también el carácter de reservado, al cual solo tendrán acceso las autoridades competentes con fines de control político, penal, disciplinario o fiscal.

10. Los libros y papeles del comerciante no podrán examinarse por personas distintas de sus propietarios o personas autorizadas para ello, sino para los fines indicados en la Constitución Nacional y mediante orden de autoridad competente. (Art. 61 del Código de Comercio).

11. La información tributaria respecto de las bases gravables y la determinación privada de los impuestos que figuren en las declaraciones tributarias, tendrá el carácter de información reservada, de conformidad con el Estatuto Tributario Colombiano.

12. Información del Registro Único de Población Desplazada (RUPD), art. 15, Decreto 2569/00.

13. Durante la instrucción, ningún funcionario puede expedir copias de las diligencias practicadas, salvo que las solicite autoridad competente para investigar y conocer de procesos judiciales, administrativos o disciplinarios, o para dar trámite al recurso de queja.

Quienes intervienen en el proceso tienen derecho a que se les expida copia de la actuación, para su uso exclusivo y el ejercicio de sus derechos. El hecho de ser sujeto procesal impone la obligación de guardar la reserva sumarial, sin necesidad de diligencia especial.

La reserva de la instrucción no impedirá a los funcionarios competentes proporcionar a los medios de comunicación información sobre la existencia de un proceso penal, el delito por el cual se investiga a las personas legalmente vinculadas al proceso, la entidad

a la cual pertenecen las personas, si fuere el caso, y su nombre, siempre y cuando se haya dictado medida de aseguramiento. (Art. 330 de la Ley 600 del 24 de julio de 2000).

14. Cuando el orden público o la seguridad nacional se vean amenazados por la publicidad de un proceso en particular, o se comprometa la preservación de la moral pública, el juez, mediante auto motivado, podrá imponer una o varias de las siguientes medidas:

a. Limitación total o parcial del acceso al público o a la prensa.

b. Imposición a los presentes del deber de guardar reserva sobre lo que ven, oyen o perciben.

15. En caso de que fuere llamada a declarar una víctima menor de edad, el juez podrá limitar total o parcialmente el acceso al público o a la prensa. (Ley 906 del 31 de agosto de 2004).

16. Cuando los intereses de la justicia se vean perjudicados o amenazados por la publicidad del juicio, en especial cuando la imparcialidad del juez pueda afectarse, el juez, mediante auto motivado, podrá imponer a los presentes el deber de guardar reserva sobre lo que ven, oyen o perciben, o limitar total o parcialmente el acceso del público o de la prensa. (Ley 906 del 31 de agosto de 2004).

17. Las audiencias preliminares deben realizarse con la presencia del imputado o de su defensor. La asistencia del Ministerio Público no es obligatoria.

Serán de carácter reservado las audiencias de control de legalidad sobre allanamientos, registros, interceptación de comunicaciones, vigilancia y seguimiento de personas y de cosas. También las relacionadas con autorización judicial previa para la realización de inspección corporal, obtención de muestras que involucren al imputado y procedimientos en caso de lesionados o de víctimas de agresiones sexuales. Igualmente aquella en la que decreta una medida cautelar. (Ley 906 del 31 de agosto de 2004).

REVISIÓN DE LEYES DE ACCESO A LA INFORMACIÓN PÚBLICA EN PERÚ Y MÉXICO

Perú

En Perú para regular el derecho fundamental de acceso a la información se expidió el 13 de julio de 2002 la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.

En ella se establece que toda información que posea el Estado se presume pública, salvo las excepciones expresamente previstas en los artículos 15, 15A y 15B de la misma.

En el derecho peruano se hace una clasificación de la información pública ante la que no se puede ejercer el derecho a la información. Dicha clasificación es como sigue:

- Información secreta (en el ámbito militar y en el ámbito de inteligencia)
- Información reservada
- Información clasificada e
- Información confidencial

Información secreta: se sustenta en razones de seguridad nacional, tiene como base fundamental garantizar la seguridad de las personas y cuya revelación originaría riesgo para la integridad territorial y/o subsistencia del sistema democrático, así como para las actividades de inteligencia y contrainteligencia.

Información clasificada en el ámbito militar: como planes de defensa militar, operaciones y planes de inteligencia y contrainteligencia militar, desarrollos técnicos o científicos propios de la defensa nacional, órdenes de operaciones, logísticas y conexas, planes de defensa de bases e instalaciones militares, material bélico, sus componentes, accesorios, operatividad o ubicación, información del personal militar.

Información clasificada en el ámbito de inteligencia: los planes estratégicos y de inteligencia, informes oficiales de inteligencia, información relacionada con el alistamiento del personal y material, actividades y planes estratégicos de inteligencia y contrainteligencia, información del personal civil o militar que desarrolla actividades de seguridad.

Información reservada: la que, por razones de seguridad nacional en el ámbito del orden interno, si se revelara originaría un riesgo a la integridad territorial o la subsistencia del sistema democrático. En consecuencia, se considera reservada la información que tiene por finalidad prevenir y reprimir la criminalidad en el país y cuya revelación puede entorpecerla.

- Los planes de operaciones policiales y de inteligencia, así como aquellos destinados a combatir el terrorismo, tráfico ilícito de drogas y organizaciones criminales.
- Las informaciones que impidan el curso de las investigaciones en su etapa policial dentro de los límites de la ley, incluyendo los sistemas de recompensa, colaboración eficaz y protección de testigos, así como la interceptación de comunicaciones amparadas por la ley, los planes de seguridad y defensa de instalaciones policiales, establecimientos penitenciarios, locales públicos y los de protección de dignatarios.
- El movimiento del personal que pudiera poner en riesgo la vida e integridad de las personas involucradas o afectar la seguridad ciudadana.

- El armamento y material logístico comprometido en operaciones especiales y planes de seguridad y defensa del orden interno.

Información clasificada: por razones de seguridad nacional y de eficacia de la acción externa del Estado, se considerará información clasificada, en el ámbito de las relaciones externas del Estado, toda aquella cuya revelación originaría un riesgo a la seguridad e integridad territorial del Estado y la defensa nacional en el ámbito externo, al curso de las negociaciones internacionales o la subsistencia del sistema democrático.

- Elementos de las negociaciones internacionales que de revelarse perjudicarían los procesos negociadores o alterarían los acuerdos adoptados, no serán públicos por lo menos en el curso de las mismas.
- Información que al ser divulgada oficialmente por el Ministerio de Relaciones Exteriores pudiera afectar negativamente las relaciones diplomáticas con otros países.

Información confidencial:

- La información que contenga consejos, recomendaciones u opiniones producidas como parte del proceso deliberativo y consultivo previo a la toma de una decisión de gobierno, salvo que dicha información sea pública.
- La información protegida por el secreto bancario, tributario, comercial, industrial, tecnológico y bursátil.
- La información vinculada a investigaciones en trámite referidas al ejercicio de la potestad sancionadora de la Administración Pública.
- La información preparada u obtenida por asesores jurídicos o abogados de las entidades de la Administración Pública cuya publicidad pudiera revelar la estrategia a adoptarse en la tramitación o defensa en un proceso administrativo o judicial, o de cualquier tipo de información protegida por el secreto profesional que debe guardar el abogado respecto de su asesorado.
- La información referida a los datos personales cuya publicidad constituya una invasión de la intimidad personal y familiar. La información referida a la salud personal se considera comprendida dentro de la intimidad personal.

México

De otra parte, en los Estados Unidos Mexicanos se expidió el 11 de junio de 2002 la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, con la cual se busca garantizar el acceso de toda persona a la información en posesión de

los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal.

En los artículos 13 a 18 de la ley mexicana se regula la información pública ante la que no se puede ejercer el derecho a la información y se clasifica como:

- Información reservada e
- Información confidencial

Para la mencionada norma la *información reservada* es aquella cuya difusión pueda:

- Comprometer la seguridad nacional, la seguridad pública o la defensa nacional.
- Menoscar la conducción de las negociaciones o bien de las relaciones internacionales, incluida aquella información que otros Estados u organismos internacionales entreguen con carácter de confidencial al Estado mexicano.
- Dañar la estabilidad financiera, económica o monetaria del país.
- Poner en riesgo la vida, la seguridad o la salud de cualquier persona.
- Causar un serio perjuicio a las actividades de verificación del cumplimiento de las leyes, prevención o persecución de los delitos, la impartición de la justicia, la recaudación de las contribuciones, las operaciones de control migratorio, las estrategias procesales en procesos judiciales o administrativos mientras las resoluciones no causen estado.

Adicionalmente establece otras especies de *información reservada*:

- La que por disposición expresa de una ley sea considerada confidencial, reservada, comercial reservada o gubernamental confidencial.
- Los secretos comercial, industrial, fiscal, bancario, fiduciario u otro considerado como tal por una disposición legal.
- Las averiguaciones previas.
- Los expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio en tanto no hayan causado estado.
- Los procedimientos de responsabilidad de los servidores públicos, en tanto no se haya dictado la resolución administrativa o la jurisdiccional definitiva.

- La que contenga las opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, hasta en tanto no sea adoptada la decisión definitiva, la cual deberá estar documentada.

La citada norma establece como *información confidencial*:

- La entregada con tal carácter por los particulares a los sujetos obligados, de conformidad con lo establecido en el artículo 19.
- Los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos de esta ley.

Estas dos iniciativas establecen contextos semejantes para la definición y distinción de la información clasificada como reservada y confidencial, que permiten establecer con claridad el alcance de las mismas y las implicaciones de su aplicación por los servidores públicos y las consideraciones propias de los impactos y sanciones ante un tratamiento inadecuado de las mismas.

IMPLICACIONES DISCIPLINARIAS EN EL TRATAMIENTO DE LA INFORMACIÓN RESERVADA: RESPONSABILIDADES Y SANCIONES

Hasta el momento hemos analizado las propuestas y consideraciones fundamentales del compartir y proteger, así como los elementos normativos tanto nacionales como internacionales que ponen de manifiesto una vista heterogénea de la información reservada y como tal su tratamiento estará sujeto a la tendencia y definición utilizada por el legislador.

Sin perjuicio de lo anterior, y comoquiera que se tienen implicaciones propias de un tratamiento inadecuado de la información reservada, a continuación revisaremos en el contexto colombiano y en la normativa internacional las responsabilidades y sanciones a las que se puede exponer un servidor público o particular en ejercicio de función pública.

La ley disciplinaria en Colombia, Ley 734 de 2002, de alcance para todos los servidores públicos y particulares en ejercicio de función pública, establece algunos deberes y prohibiciones frente a la información a la cual por el ejercicio de empleo, cargo o función tiene acceso dicho funcionario, que como hemos podido observar y detallar en la guía enunciativa (previamente revisada) se advierten al menos 17 tipos de información con declaraciones de reserva.

Si bien no tenemos una definición homogénea de la información reservada, la conducta del servidor público se agravará por un inadecuado tratamiento de dicha información,

toda vez que este se obliga al estricto cumplimiento de la Constitución y la ley como se advierte en el numeral 1.º del artículo 34 de la ley disciplinaria.

Así las cosas, se enumeran a continuación algunos deberes y prohibiciones consignadas en los artículos 34 y 35 de la Ley 734 de 2002, que se deben analizar frente al tratamiento de la información reservada en el sector público.

Artículo 34. Deberes:

(...)

4. Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos.

5. Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos.

(...)

Artículo 35. Prohibiciones:

(...)

13. Ocasionar daño o dar lugar a la pérdida de bienes, elementos, expedientes o documentos que hayan llegado a su poder por razón de sus funciones.

(...)

21. Dar lugar al acceso o exhibir expedientes, documentos o archivos a personas no autorizadas.

(...)

Adicionalmente se tiene en el artículo 48 del Código Único Disciplinario una falta gravísima que, en conjunto con el 269F de la ley penal en temas informáticos, exige de los servidores públicos un debido cuidado no solo con la información reservada, sino con la protección de los datos personales, toda vez que dichas faltas se sancionan con destitución e inhabilidad para el ejercicio de función pública mínimo por 10 años:

(...)

43. Causar daño a los equipos estatales de informática, alterar, falsificar, introducir, borrar, ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos o en los que se almacene o guarde la misma, o permitir el acceso a ella a personas no autorizadas.

(...)

Adicionalmente, en el proyecto de ley de acceso a la información pública, se establecen responsabilidades penales, civiles y disciplinarias, que son mencionadas a continuación. La citada norma establece en sus artículos 44, 45 y 46 dichas responsabilidades como sigue:

Artículo 44. Responsabilidad penal y disciplinaria/civil. Un acto de buena fe en el ejercicio, cumplimiento o intención de cumplimiento de una competencia o deber en los términos de la presente Ley no podrá ser considerado delito ni falta disciplinaria, siempre que se haya actuado razonablemente.

Artículo 45. Responsabilidad penal. Todo acto de ocultamiento, destrucción o alteración deliberada total o parcial de información pública, una vez haya sido objeto de una solicitud de información, será sancionado en los términos del artículo 292 del Código Penal.

Artículo 46. Responsabilidad disciplinaria. Configuran una infracción disciplinaria gravísima las siguientes conductas, cuando se realicen en forma intencional, y podrán ser disciplinadas internamente por el sujeto obligado o puestas en conocimiento de la Procuraduría, quien en todo caso podrá ejercer el poder disciplinario preferente:

- a) Obstruir el acceso a cualquier documento en forma contraria a lo dispuesto en esta Ley;
- b) Impedir el cumplimiento de las obligaciones dispuestas en esta Ley a un sujeto obligado; y
- c) Obstaculizar el trabajo de la Comisión Nacional para la Transparencia y el Acceso a la Información Pública. Cualquier persona puede denunciar ante la Comisión de una de las infracciones administrativas definidas anteriormente.

Parágrafo. Toda sanción que se imponga deberá ser anunciada en el sitio web de la Comisión y del sujeto obligado respectivo y en defecto de la existencia de un sitio web, en los dispositivos de divulgación existentes en su dependencia, dentro del plazo de cinco (5) días a partir de su imposición.

Llama la atención la anotación del artículo 44 sobre “un acto de buena fe en el ejercicio, cumplimiento o intención de cumplimiento o deber ...”, que deja un espacio abierto para valorar las acciones de un servidor público frente al tratamiento de la información, lo cual, sin un adecuado conjunto de prácticas de protección de información claramente establecido, genera un contexto de subjetividad y posible impunidad toda vez que la prueba de la buena fe puede ser inadecuada sin tener en consideración aquellas acciones que previamente se tengan definidas para proteger la misma.

De otra parte, la sanción disciplinaria prevista en el artículo 46 se advierte como falta gravísima, engrosando la ya extensa lista de faltas de este tipo registradas en el artículo 48 de la ley disciplinaria. Nótese que el texto del artículo 46 habla de “(...) cuando se realicen en forma intencional (...)”, lo que nuevamente requiere un ejercicio probatorio especializado que permita con claridad establecer la intencionalidad de hecho. Esto es, sin un conjunto de directrices y acciones establecidas bien en un procedimiento o lineamiento sobre el manejo de la información para su adecuado tratamiento, las validaciones que se hagan al respecto estarán basadas en el análisis de actuaciones propias del servidor público y no de prácticas claras para el cumplimiento de su deber de protección de la información.

En el contexto internacional, tanto en Perú como en México, en sus respectivas leyes de acceso a la información pública, se tienen previstas sanciones por el incumplimiento de dicha norma, que no es otra cosa que el inadecuado tratamiento de la información bien reservada o confidencial.

En la norma peruana se lee:

Artículo 4°. Responsabilidades y sanciones:

Todas las entidades de la Administración Pública quedan obligadas a cumplir lo estipulado en la presente norma.

Los funcionarios o servidores públicos que incumplieran con las disposiciones a que se refiere esta Ley serán sancionados por la comisión de una falta grave, pudiendo ser incluso denunciados penalmente por la comisión de delito de Abuso de Autoridad a que hace referencia el Artículo 377° del Código Penal.

El cumplimiento de esta disposición no podrá dar lugar a represalias contra los funcionarios responsables de entregar la información solicitada.

De igual forma, en la norma mexicana se tiene:

Artículo 63. Serán causas de responsabilidad administrativa de los servidores públicos por incumplimiento de las obligaciones establecidas en esta Ley las siguientes:

- Entregar información considerada como reservada o confidencial conforme a lo dispuesto por esta Ley.

La responsabilidad a que se refiere este Artículo o cualquiera otra derivada del incumplimiento de las obligaciones establecidas en esta Ley, será sancionada en los términos de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos. (...) la reincidencia (...) serán consideradas como graves para efectos de su sanción administrativa.

Artículo 64. Las responsabilidades administrativas que se generen por el incumplimiento de las obligaciones a que se refiere el Artículo anterior, son independientes de las del orden civil o penal que procedan.

Si bien en cada una de las normas citadas se establecen elementos concretos del incumplimiento de un deber funcional de protección de la información reservada, el servidor público también debe contar con elementos para orientar su conducta, efectuar un tratamiento adecuado de la información y asegurar el cumplimiento de la ley, siendo tales elementos los que se echan de menos en la legislación y doctrina colombianas, ya que en las mismas no hay una unificación de criterios para el manejo correcto y responsable de la información, de modo que el servidor se ve en conflicto frente al manejo de la información porque no se le brindan herramientas para determinar en qué casos o sobre qué información se puede predicar la reserva o la publicidad.

Así las cosas, si bien el servidor tiene conocimiento de la conducta que lo haría incurrir en falta disciplinaria, no conoce los aspectos conforme a los cuales debe actuar y los lineamientos para la ponderación de los derechos fundamentales como el derecho a la intimidad, honra y buen nombre, o las necesidades de protección de la información por razones de seguridad nacional, todo ello en contraposición al derecho a la información y la libertad de expresión, atendiendo además a la obligación del servidor de responder de fondo las solicitudes de información, ya que el derecho de petición también es fundamental³³ y por lo mismo requiere ser tenido en consideración al momento de resolver requerimientos de información y documentos que estén sometidos a reserva o sean reservados.

33 Constitución Política de Colombia. Artículo 23: “Toda persona tiene derecho a presentar peticiones respetuosas a las autoridades por motivos de interés general o particular y a obtener pronta resolución. El legislador podrá reglamentar su ejercicio ante organizaciones privadas para garantizar los derechos fundamentales”.

LINEAMIENTOS Y PRÁCTICAS DE ASEGURAMIENTO DE LA INFORMACIÓN RESERVADA

Habida cuenta de que en el ejercicio de la función pública son muchos los momentos en los cuales se tiene acceso a información reservada o sometida a la reserva, se hace necesario un adecuado tratamiento para dar cumplimiento a los deberes y obligaciones que se derivan de este acceso, so pena de incurrir en faltas o sanciones que implican indefectiblemente afectación de derechos fundamentales.

Así las cosas, en esta sección del documento se sugiere un conjunto base de prácticas de seguridad y control que permitan avanzar en un tratamiento de la información reservada o sometida a la reserva, a la que, por el ejercicio de su cargo, los servidores públicos tengan acceso. Para ello, seguiremos algunas ideas propuestas por SHAW³⁴, GÓMEZ VIETES³⁵ y CANO³⁶ como referentes básicos revisados en una perspectiva integrada entre privacidad y seguridad de la información, así como elementos conceptuales propios de la protección de la información como soporte a los lineamientos expuestos por las buenas prácticas internacionales, ello desde el ámbito empresarial y tecnológico.

SHAW establece un ciclo de vida para la privacidad y la seguridad de la información, como una forma de establecer un tenor concreto de las responsabilidades, exigencias y cumplimiento que las organizaciones deben considerar cuando de atender las obligaciones, riesgos y tratamiento de la información se requiere, no solo para verificar que se consideran las regulaciones del caso, sino para comprender que tanto la seguridad como la privacidad son disciplinas complementarias, que hacen de su aplicación una forma de elevar la confianza de los grupos de interés frente a sus objetivos empresariales.

El ciclo planteado establece cinco pasos:

1. Identificar y revisar los estatutos y regulaciones aplicables a la organización.

Este primer paso demanda que las organizaciones cuenten con un observatorio permanente de regulaciones y leyes de cada una de las regiones o sectores donde opera la empresa, de tal forma que desarrolle un diagnóstico concreto sobre las condiciones actuales de su cumplimiento frente a las prácticas corporativas respecto del tema.

34 SHAW, T. *Information security and privacy. A practical guide for global executives, lawyers and technologists*, American Bar Association (ABA), Section of Science and Technology, 2011.

35 GÓMEZ VIETES, A. *Enciclopedia de la seguridad informática*, 2ª ed., Ra-Ma, 2011.

36 CANO, J. *Inseguridad de la información. Una visión estratégica*, Alfaomega, 2013.

2. Identificar y analizar las fuentes potenciales de responsabilidad.

Esta fase pretende que la organización establezca un análisis exhaustivo de activos de información regulados existentes, que permita determinar el alcance de las responsabilidades y el ejercicio de controles requerido por la empresa. Esta identificación pasa por el análisis de *hardware*, *software*, aplicaciones (ambientes de pruebas, calidad y producción), redes y facilidades que las empresas utilizan para la transmisión de datos, propietarios y custodios de información.

3. Aplicación de políticas y valoraciones de riesgos.

Por un lado, esta etapa busca revelar las políticas de seguridad y control de la organización y cómo estas son aplicadas y verificadas en el contexto del inventario de activos de información regulados previamente identificado. De igual forma, este marco de actuación frente a la protección de la información debe contar con un tono claro de la gerencia, que imprima la relevancia del tema en las agendas estratégicas de los ejecutivos de primer nivel, así como en la cultura de sus empleados. Así mismo, las valoraciones de riesgo deben mantener una vista integrada del nivel de exposición de la organización frente a eventos de falla parcial o total, con el fin de mantener una postura proactiva frente a las amenazas y vulnerabilidades que puedan afectar el modelo de generación de valor del negocio.

4. Diseño, aplicación y validación de los controles de seguridad y privacidad de la información.

Una vez identificados los riesgos y sus impactos sobre los activos de información relevantes para la empresa, se hace necesario identificar o diseñar las medidas de mitigación de los mismos y asegurar la efectividad de estas. En particular, se cuenta con listas de controles generalmente aceptados en documentos como:

* NIST *Special publication 800-53. Recommended security controls for Federal Information Systems and Organizations.*

* ISO 27002.

* COBIT de ISACA.

En particular en esta etapa se requiere una especial coordinación entre los objetivos de los controles que se seleccionen, de tal forma que se ajusten tanto a las necesidades de privacidad como a las de seguridad, considerando que el mínimo de controles que se apliquen ofrezcan una vista estandarizada, confiable y verificable del ambiente de control requerido para los datos claves de la empresa.

5. Asegurar el cumplimiento, los procesos de auditoría y certificación.

Una vez implementado el conjunto mínimo de controles y su uso en la operación diaria de la empresa, estos deben ser monitoreados y verificados frente a los objetivos de seguridad y privacidad de la empresa, así como de los requisitos legales de cumplimiento normativo nacional o internacional. Para ello, esta fase exige un seguimiento y reporte periódico de monitoreo interno de la efectividad de los controles, sin perjuicio de evaluaciones y auditoría externas que se planteen por parte de entes de supervisión y vigilancia para conocer el estado del modelo de seguridad, control y privacidad de la organización.

Por su parte, GÓMEZ VIETES establece una sugerencia de clasificación de información que aclara el panorama de las responsabilidades del tratamiento de la información, sabiendo que aquella que reviste la menor confidencialidad será la que contará con menos prácticas de seguridad y control, dados sus impactos ante una falla total o parcial que implique pérdida o fuga de la misma. En este sentido, el investigador detalla³⁷:

- Información sin clasificar o desclasificada: podría ser conocida por personas ajenas a la empresa.
- Información de uso interno: conocida y utilizada solo por empleados de la organización, así como algún colaborador externo autorizado. No obstante, no conviene que esta sea divulgada a terceros.
- Información confidencial: solo puede ser conocida y utilizada por un determinado grupo de empleados. Su divulgación podría ocasionar daños significativos a la organización.
- Información reservada (o secreta): solo puede ser conocida y utilizada por un grupo muy reducido de empleados (generalmente directivos de la empresa). Su divulgación puede ocasionar graves daños a la organización, *incluso multas y/o sanciones*. (Las *cursivas* están fuera del texto original).

Continúa el académico indicando que “una vez definida la clasificación, será necesario proceder al marcado o etiquetado de la información”, lo cual indica y advierte sobre el tratamiento que se le debe dar durante su ciclo de vida, es decir, desde su creación, uso, almacenamiento, transporte, recuperación y disposición final.

De manera complementaria, GÓMEZ VIETES establece en su libro que la organización debe mantener una base de datos con el registro de la información más sensible, registrando su fecha de creación, la utilización prevista, la fecha de destrucción, el cambio

37 GÓMEZ VIETES, 2011, p. 112.

de clasificación del documento, propietario, usuarios, etcétera. Así mismo, de cada acceso a esta información sensible deberá quedar como mínimo la identificación del usuario, la fecha, la hora, la información a la cual se accede, el tipo de acceso (lectura, escritura, actualización) y nivel de autorización.

A nivel de técnicas de protección de datos, se establece que la información más sensible, en este caso siguiendo la clasificación previamente detallada, la confidencial y reservada, deberá asegurar el uso de algoritmos de cifra que permitan mantener las exigencias de secreto pretendidas por su nivel de confidencialidad. En este sentido, podríamos establecer que la información clasificada como confidencial y secreta, si no está en uso y se encuentra en formato electrónico, debería estar cifrada o codificada a fin de prevenir que pueda ser conocida o revelada por terceros no autorizados.

De manera complementaria, CANO, siguiendo las indicaciones de SMALLWOOD³⁸ contenidas en un informe de Forrester Research, propone algunos patrones de diseño asociados con la seguridad de la información, válidos tanto en un contexto móvil como local, que permiten a la organización disminuir la probabilidad de pérdida o fuga de información. Las indicaciones son:

Uso de clientes delgados: esta consideración establece acceso a la información en línea, sin operación o manejo local, donde no existe almacenamiento de datos, documentos o programas, manteniendo la información clasificada como confidencial almacenada y custodiada de manera central.

Uso de dispositivos delgados: estos dispositivos deben ser configurados para efectuar consultas de los documentos originales y mantener copias que no pueden ser modificadas o alteradas. Adicionalmente se recomienda poder configurar la posibilidad de borrar o eliminar la información de manera remota ante eventos de pérdida del dispositivo.

Almacenamiento protegido: consiste en tener en el equipo de escritorio (que generalmente no es propiedad de la organización y tampoco es controlado por esta) una partición local protegida donde se almacenan los documentos electrónicos, para ser procesados de manera segura y controlada. Este patrón permite una operación local, operación fuera de línea, administración central, seguridad granular a nivel de documento y borrado remoto de ser necesario.

Datos protegidos: desarrollar un programa de *information right management* (IRM) embebido dentro de los documentos o datos con el fin de proveer un ciclo de vida de documento seguro. Esto es, los derechos de acceso sobre los datos dependen del con-

38 SMALLWOOD, R. *Safeguarding critical e-documents. Implementing a program for securing confidential information assets*, John Wiley & Sons, 2012.

texto, es decir, de dónde y cuándo un usuario puede tener acceso. Por ejemplo, se quiere que tenga acceso en su computador de escritorio, en las horas laborales.

Uso de tecnologías de prevención de fuga de información: establecer el uso de tecnologías como *data loss prevention* (DLP) para revisar el contenido del tráfico de redes y controlar el flujo de documentos confidenciales o con datos sensibles en el perímetro. Esto es, desde el punto final (equipos de cómputo personales), pasando por el correo electrónico y los servidores corporativos. Es de anotar que este tipo de soluciones son complementarias a las medidas de protección de la información que tenga la empresa.

Todas estas consideraciones son posibles siempre y cuando se asegure una práctica de clasificación de información, la cual exige una reconversión de la cultura de protección de la información en los individuos, donde cada uno se vea como custodio de sus datos y, por lo tanto, responsable por su adecuado tratamiento.

PERSPECTIVAS Y REFLEXIONES FINALES

Teniendo en cuenta las divergencias tanto desde los puntos de vista teórico, fáctico y práctico, en cuanto al conflicto entre los derechos a la intimidad, la honra, el buen nombre, y el derecho a la información, a la libertad de expresión y la necesidad de mantener la seguridad nacional en relación con la publicidad o reserva de la información, se advierte que tanto la Corte Constitucional colombiana como la Corte Interamericana de Derechos Humanos han ponderado la necesidad de protección de los mismos en cada caso concreto, pero a su vez planteando lineamientos para el abordaje general del tema, conforme a los cuales, y teniendo en cuenta lo antes expuesto, se observa que existen dos grandes frentes en los que se mueve la información y su necesidad de protección o de publicidad; estos son: el ámbito privado o particular y el ámbito público o estatal.

En relación con la información privada, particular o personal, jurisprudencialmente se ha señalado que rige la regla de la reserva como medio de protección a los derechos a la intimidad, la honra y el buen nombre, por considerar que es necesario evitar el mal uso de la información privada de las personas en sus diferentes grados de intimidad (personal, familiar, social e incluso gremial)³⁹, en el entendido que el particular es propietario de su propia información y, en consecuencia, es quien puede decidir sobre su difusión y publicidad, que en este caso son la excepción, por lo que solamente podría ser posible sacrificar ese derecho a la intimidad por razones superiores⁴⁰, esto es, de índole social o de interés general y con base en el derecho a la información y a la liber-

39 Corte Constitucional. Sentencia T-303 de 2008. Expediente T-1.791.986. Decisión del 3 de abril de 2008. M.P.: MARCO GERARDO MONROY CABRA.

40 Corte Constitucional. Sentencia T-1025 de 2007. Expediente T-1.401.460. Decisión del 3 de diciembre de 2007. M.P.: MANUEL JOSÉ CEPEDA ESPINOSA.

tad de expresión y solamente cuando haya necesidad de ello por la prevalencia de la libertad de expresión en cuanto al debate de asuntos públicos o de interés colectivo⁴¹.

De este modo, y en atención al reconocimiento superior de los derechos humanos y los derechos fundamentales, de los cuales hacen parte la dignidad humana y el derecho a la intimidad personal, en el escenario de la información privada, lo general es la reserva de la información y la excepción es la publicidad, y esta última solamente tiene dos matices que son la voluntad de la persona para divulgar su propia información, y la necesidad superior de la colectividad, lo cual estaría sometido a la ponderación de quien requiere hacer pública esa información, que no podría ser otro que el Estado por medio de sus diferentes estamentos en los cuales se congrega la información privada de las personas, *v. gr.*, las bases de información de historias clínicas.

A su turno, la Corte Interamericana de Derechos Humanos, en su jurisprudencia, ha establecido un test para determinar en qué casos es posible la limitación al derecho a la libertad de expresión consagrado en el numeral 13 de la Convención Americana de Derechos Humanos como el “derecho de toda persona a la libertad de pensamiento y de expresión, y comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole”⁴², de modo que involucra el derecho a la información y por consiguiente la información pública, pues el ejercicio de tal derecho “no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar: (a) el respeto a los derechos o a la reputación de los demás, o (b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas”⁴³; así, se exige que las restricciones se determinen en forma clara y precisa en una ley, que se dirija a la consecución de objetivos imperiosos reconocidos por la Convención Americana de Derechos Humanos y que sean necesarias en una sociedad democrática, así como que se justifiquen frente a la restricción de la libre expresión⁴⁴.

De igual forma, se ha señalado que si la ley que determina la restricción es vaga o ambigua, puede generar que haya actos de arbitrariedad como la censura previa, que por miedo a las sanciones se evite la difusión de la información y de las opiniones o que mediante decisiones judiciales se restrinja en forma indebida la libertad de expresión, por lo cual no se debe dar lugar a mayores interpretaciones, ni siquiera de índole judicial⁴⁵.

41 “El derecho de acceso a la información en el marco jurídico interamericano”. Relatoría Especial para la Libertad de Expresión. Comisión Interamericana de Derechos Humanos. 2010. Disponible en: www.cidh.org/relatoria

42 *Ibídem.*

43 *Ibídem.*

44 *Ibídem.*

45 *Ibídem.*

Ahora bien, en relación con la información pública o estatal, se advierte cómo la regla general es la publicidad⁴⁶ o el acceso público porque ello permite el control de la gestión pública⁴⁷, y la excepción es la reserva; sin embargo, en torno al tema la Corte Constitucional ha realizado avances en cuanto a los criterios para definir ese acceso a la información o documentos públicos, considerando que sobre el tema existe la primacía del derecho a la información, definido⁴⁸ como “*aquel derecho fundamental que tiene toda persona a ser informada y a informarse de la verdad, para juzgar por sí misma sobre la realidad con conocimiento suficiente*”, y que ello “*se encuentra en relación estrecha con el derecho al acceso a documentos públicos*”, como formas del principio de publicidad que se rige, entre otras, por lo establecido en la Ley 57 de 1985.

A su vez, se ha elaborado el “Estudio especial sobre el derecho de acceso a la información”, de la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, en el año 2007, señalando que el derecho a la información se refiere a la información en general, que el Estado está obligado a suministrarla excepto que se trate de información personal; es un derecho de titularidad universal, por lo que no hay obligación de acreditar un interés directo o una afectación personal para solicitarla en cuanto se trate de información pública; por esta razón, se estableció el derecho de petición consagrado en el artículo 23 de la Constitución Política de Colombia y regulado en el Código Contencioso Administrativo como el medio para la consecución sencilla y rápida de la información y la acción de tutela para garantizar tal derecho cuando se niegue información con fundamento en aspectos diferentes a la reserva constitucional, legal, o por motivos de seguridad nacional, ello en forma adicional al recurso de insistencia para permitir el acceso a la información cuando es negada por la autoridad competente con base en las razones legítimas que dan lugar a la existencia de la restricción⁴⁹.

De conformidad con lo expuesto, se tiene que la restricción del principio de publicidad o reserva de la información, solamente puede ocurrir por mandato legal o cuando se trate de información relacionada con la defensa y seguridad nacional, con base en criterios de razonabilidad y publicidad, sin que pueda haber discrecionalidad, sino que solamente existe reserva cuando una ley así lo exprese, y dicha reserva debe darse únicamente por un tiempo determinado, pues debe terminar en algún momento para

46 Corte Constitucional. Sentencia T-690/07. Expediente T-1606748. Decisión del 4 de septiembre de 2007. M.P.: NILSON PINILLA PINILLA.

47 Corte Constitucional. Sentencia C-872/03. Expediente D-4537. Decisión del 30 de septiembre de 2003. M.P.: CLARA INÉS VARGAS HERNÁNDEZ.

48 Corte Constitucional. Sentencia T-705/07. Expedientes T-1613624, T-1613625, T-1613626, T-1613627 acumulados. Decisión del 7 de septiembre de 2007. Magistrado ponente: JAIME CÓRDOBA TRIVIÑO; y sentencia C-488 de 1993. Expediente D-272. Decisión del 28 de octubre de 1993. M.P.: VLADIMIRO NARANJO MESA.

49 Corte Constitucional. Sentencia T-1025 de 2007. Expediente T-1.401.460. Decisión del 3 de diciembre de 2007. M.P.: MANUEL JOSÉ CEPEDA ESPINOSA.

que la información pueda pasar a ser de dominio público; además, se debe motivar debidamente la reserva de la información y la persona solicitante de la información debe costear su obtención (copias o grabación, por ejemplo); es un deber del servidor público el fundamentar debidamente la negación de la información, expresando la norma en que se funda la reserva, sabiendo que puede haber controles disciplinarios, administrativos y judiciales al respecto.

En relación con la forma en que la ley debe establecer la reserva, se ha señalado que debe indicarse “(i) el tipo de información que puede ser objeto de reserva, (ii) las condiciones en las cuales dicha reserva puede oponerse a los ciudadanos, (iii) las autoridades que pueden aplicarla y (iv) los sistemas de control que operan sobre las actuaciones que por tal razón permanecen reservadas”⁵⁰.

Sobre la reserva por la protección de la información relacionada con la defensa y seguridad nacional, se tiene que se incluye en ese espectro la seguridad nacional, el orden público y la salud pública, y a su vez se establece la reserva para asegurar la eficacia de las investigaciones estatales de carácter penal, disciplinario, aduanero o cambiario y para garantizar secretos comerciales e industriales.

Además, se ha señalado que la reserva solamente opera en cuanto al contenido de los documentos y no a su existencia, y la relacionada con procesos públicos no puede operar sobre todo el proceso en que cursa la información reservada.

Establecidos entonces los aspectos en que existe reserva, se tiene que la jurisprudencia también ha establecido que el Estado debe informar sobre su gestión, generando a su vez la custodia de la información reservada para que al terminar el periodo de la restricción se haga posible su publicidad y que la información esté en buen estado para ello, aspecto en el cual entran a jugar un papel decisivo los medios de conservación de documentos físicos y digitales, a fin de que se proteja debidamente la información.

Por otra parte, y desde la óptica de la tecnología y las empresas, GARTNER⁵¹ advierte en un reciente estudio, publicado por uno de sus analistas en abril de 2012, que la información y la tecnología serán usadas de manera agresiva por los líderes de empresariales e individuos para repensar los parámetros actuales de los modelos de negocio y generar una ambiciosa colaboración entre las personas, para crear conceptos más allá de lo que el mundo real nos puede ofrecer.

En este escenario, no es posible detener el uso de tecnologías móviles, de los servicios de información instantánea ni la natural progresión de las empresas hacia la estrategia

50 Corte Constitucional. Sentencia T-511 de 2010. Expediente T-2.395.898. Decisión del 18 de junio de 2010. M.P.: HUMBERTO ANTONIO SIERRA PORTO.

51 MAHONEY, J., MORELLO, D. y ROBERTS, J. Exploring the future: Everyone's IT. *Gartner Research*, 2012.

en la nube, pero sí identificar de manera selectiva aquella información y áreas claves de las empresas y los estados en las cuales, luego de un ejercicio consciente y estructural basado en riesgos e impactos, se requiere balancear la necesidad de protección con la exigencia de compartir.

La tensión entre los conceptos se presenta siempre que se contraponen las necesidades corporativas y estatales de visibilidad y presencia en internet, con las exigencias de los mercados y las prácticas de industria frente a la información, que articulan en sí mismas dos condiciones relevantes para empresas y gobiernos del siglo XXI, la transparencia y la rendición de cuentas, con la protección del valor y la generación de ventajas competitivas con el uso de la información.

Bien anotan los especialistas en estrategia que todo aquello que hoy ha sido exitoso y relevante para el logro de los objetivos empresariales, mañana terminará indefectiblemente convertido en un *commodity*, algo que puede ser claramente copiado y superado, y que en corto plazo no será un diferenciador empresarial, sino algo que se requiere para competir⁵².

En este contexto, las reflexiones sobre la tensión entre el compartir y proteger adquieren una dimensión particularmente estratégica, pues en el ejercicio de conocer aquello que resulta importante para la estrategia empresarial (o gubernamental) y la rendición de cuentas a terceros, la información juega un papel relevante que explica la relevancia de la organización en la dinámica del tejido empresarial y nacional.

Así las cosas, las tensiones aumentan cuando los mercados demandan negocios innovadores y quebrantamiento de reglas, los cuales necesariamente implican análisis de información de grandes datos, inteligencia de negocios y analítica especializada, que claramente genera conocimiento y condiciones novedosas que articulan una nueva forma de intervenir el entorno, posiblemente cambiándolo⁵³. Por lo tanto, la esencia del compartir estará mediada por la idea del proteger, pues la supervivencia de la empresa y del Estado juega un papel relevante ante el desarrollo de una posición estratégica privilegiada de esta.

Ahora bien, en un mundo dominado por la información y la necesidad de anticipación a los eventos futuros, es natural que los ciudadanos conozcan la realidad de la empresa frente a sus retos venideros; es decir, que las organizaciones y naciones ejerzan su gobierno corporativo haciendo transparentes sus procedimientos y resultados frente a sus grupos de interés. En razón con lo anterior, se exacerba la necesidad de compartir y

52 HAX, A. *El modelo delta. Un nuevo marco estratégico*, 2003. Disponible en: <http://cirpq.tripod.com/consultoriaestrategica/modelodelta.pdf> (consultado: 21-05-2012).

53 HAMEL, G. *Lo que importa ahora. Cómo triunfar en un mundo de cambios implacables, competencia feroz e innovación sin barreras*, Norma, 2012.

revelar información frente a la de proteger y restringir, toda vez que las bondades del ejercicio de gobierno generan confianza inversionista y un ambiente propicio para integrar los impactos sociales y las exigencias corporativas y nacionales.

Por consiguiente, cuando la motivación de transparencia se haga más evidente y requerida por los grupos de interés, la esencia del proteger estará mediada por la de compartir, esto es, la información deberá ser revelada conforme a los acuerdos establecidos con las comunidades, sin mancillar la protección de la reputación corporativa y del gobierno, que si bien se verá enaltecida con la rendición de cuentas, deberá ser asistida con la reserva de la información relevante para proteger su viabilidad en el futuro.

En este ejercicio de revisión de dichas tensiones entre el proteger y compartir, en el contexto de la información reservada o sometida a la reserva, se encontró que en el ordenamiento jurídico colombiano no existe una norma compiladora de todas las disposiciones que enlisten taxativamente la información que ha sido declarada a través de la Constitución y la ley; en consecuencia, para saber si un documento o cierta información es reservada, es necesario realizar una revisión integral del ordenamiento jurídico, que por las características de ser extenso, disperso y por momentos confuso, hace de esta revisión una verdadera pesquisa que demuestra la falta de homogeneidad en el tema.

En este sentido, los servidores públicos y particulares en el ejercicio de función pública deben recorrer el ordenamiento jurídico buscando las consideraciones más relevantes para asegurar un cumplimiento acertado de su deber funcional de protección de la información reservada o sometida a la reserva, que, sin referentes concretos de prácticas de seguridad y control, los exponen a responsabilidades y sanciones disciplinarias que comprometen en la mayoría de las ocasiones derechos fundamentales.

Frente a esta situación se proponen en este documento algunos lineamientos y prácticas de seguridad y control que permitan a los servidores públicos contar con elementos concretos para cumplir con el deber de protección de información propio del ejercicio de su cargo, para que en el evento de realizarse alguna conducta que materialice la ilicitud sustancial, el proceso disciplinario cuente con referentes que permitan establecer el grado de imperfección de la comisión de los hechos y no se lance a una búsqueda de posibilidades que pueden no ser ajustadas a la realidad del ejercicio de los deberes propios del cargo del servidor público.

Así las cosas, resolver la tensiones entre el proteger y compartir será un ejercicio de tensión creativa y prácticas de seguridad y control que lleve a las organizaciones públicas y privadas a encontrar el justo medio de los griegos, que descubra la virtud que cumpla con la necesidad de ejercitar el gobierno empresarial y su responsabilidad con sus grupos de interés y la legítima defensa de sus intimidades estratégicas y de negocio para mantener su rumbo en el cumplimiento de sus metas grandes y ambiciosas.

BIBLIOGRAFÍA

BROTBY, K. *Information security governance*, Hoboken, New Jersey, John Wiley and Sons, 2009.

CANO, J. *Inseguridad de la información. Una visión estratégica*, Bogotá, Alfaomega, 2013.

FOSTER, C. Sharing or controlling? Examining the decision to segregate information within the organization. *ISACA Journal*, vol. 2, 2012.

GANTZ *et al.* The diverse and exploding digital universe. *IDC Research*, 2008. Disponible en: www.emc.com/collateral/analyst-reports/diverse-exploding-digital-universe.pdf (consultado: 21-05-2012).

GÓMEZ VIETES, A. *Enciclopedia de la seguridad informática*, 2ª ed., Madrid, Ra-Ma, 2011.

HAMEL, G. *Lo que importa ahora. Cómo triunfar en un mundo de cambios implacables, competencia feroz e innovación sin barreras*, Bogotá, Norma, 2012.

HAX, A. *El modelo delta. Un nuevo marco estratégico*, 2003. Disponible en: <http://cirpq.tripod.com/consultoriaestrategica/modelodelta.pdf> (consultado: 21-05-2012).

MAHONEY, J., MORELLO, D. y ROBERTS, J. Exploring the future: Everyone's IT. En: *Gartner Research*, 2012.

SHAW, T. *Information security and privacy. A practical guide for global executives, lawyers and technologists*, Chicago, American Bar Association, ABA. Section of Science and Technology, 2011.

SMALLWOOD, R. *Safeguarding critical e-documents. Implementing a program for securing confidential information assets*, Hoboken, New Jersey, John Wiley & Sons, 2012.