En el contexto de la era de la información, el ser humano es y será lo que reflejen sus datos personales o lo que se interprete de los mismos.

Censos, estadísticas y datos personales en la era del gobierno electrónico:

Nelson Remolina Angarita·

Abstract

The protection of human rights against the improper use of sophisticated information technology is a problem that remains unsolved. Each day new sophisticated information technologies create modern and previously unimaginable ways to challenge the protection of human rights. Modern computing technologies and the Internet have generated the capacity to gather, manipulate, and share massive quantities of data.

Data protection governs the manner in which computerised data relating to individuals may be collected, held, processed, used, disclosed and transferred. Throughout this article the reader will be introduced to the key elements which go towards an understanding of data protection law with specially reference to the personal data collected by the government for census and statistical purposes.

Resumen

El artículo analiza los principales aspectos relacionados con la protección de datos personales en el sector público con particular referencia al tratamiento de información personal que se recolecta con ocasión de los censos y encuestas. Se precisan algunos riesgos que genera el uso inadecuado de esta información y se resumen ciertos aspectos fundamentales relacionados con la regulación internacional del dato estadístico y la reserva estadística. Finalmente, se plantean algunas sugerencias para el caso colombiano.

KEY WORDS: Dato estadístico; censos; encuestas; gobierno electrónico; Habeas data; data protection; dato personal; tratamiento de datos personales; bases de datos; reserva legal; acceso a información.

· Abogado y Especialista en Derecho Comercial de la Universidad de los Andes. Master of Laws del London School of Economics and Political Sciences. Profesor de Planta de la Facultad de Derecho de la Universidad de los Andes. Fundador y Director del GECTI de la Facultad de Derecho de la Universidad de los Andes (Bogotá, Colombia). nremolin@uniandes.edu.co

I.- Introducción

Los avances tecnológicos de información permiten realizar cualquier tipo de operación sobre la información acerca de una persona (dato personal): recolección, acceso, interrelación, interconexión, almacenamiento, análisis, circulación –nacional e internacional- entre otros. Por eso, las entidades estatales y los particulares han venido incrementando el uso de las tecnologías y los datos personales para múltiples finalidades. Adicionalmente, la información sobre las personas se ha convertido en un bien permanentemente comercializado y en un insumo diario de los sistemas de información privados y gubernamentales. De hecho, los datos personales son el principal activo de algunas empresas.

Con ocasión del uso de las tecnologías de la información en prácticamente todas las actividades, nos venimos familiarizando con nuevos términos como comercio electrónico y gobierno electrónico, entre otros. En uno y otro, el tratamiento[1] de datos personales juega un rol esencial. La actividad gubernamental respecto del uso de este tipo de información no debe amenazar ni vulnerar los derechos humanos y las libertades individuales.

Los censos se han convertido en una fuente de recolección masiva de información de la que hacen uso los gobiernos para diferentes finalidades. Para el 2005 se ha anunciado la implementación en Colombia del XVII Censo Nacional de Población y VI de Vivienda. Se censarán a todas y cada una de las personas, hogares y viviendas en todo el territorio nacional. A través del mismo se recogerá, recopilará, evaluará, analizará y divulgará datos demográficos, económicos, sociales y estadísticos correspondientes a todos los residentes y sus viviendas. Mediante el censo se busca, entre otros, obtener información actualizada, oportuna y confiable sobre la población total del país, su distribución espacial, a nivel de regiones, departamentos, municipios y localidades, así como sus características demográficas básicas. Adicionalmente, la información permitirá determinar las características de los hogares, saber cómo es su conformación y las condiciones que viven sus integrantes.

El censo implica la recolección de mucha información sobre millones de ciudadanos. Desde la óptica jurídica, éste está estrechamente ligado a la protección de datos personales la cual ha cobrado un espacio importante a partir de la consagración del habeas data y de la libertad informática en el artículo 15 de la Carta Política

1 A efectos del presente documento, esta expresión se entenderá como cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recolección, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

colombiana de 1991. Como quiera que el tratamiento inadecuado de datos personales puede generar la vulneración de algunos derechos fundamentales y libertades individuales (intimidad, información, buen nombre, igualdad, honra, honor, libertad, entre otros) y ser nicho de usos no autorizados e ilegales, el presente documento busca analizar las implicaciones jurídicas sobre el uso de datos personales en el sector público con especial referencia a la información recolectada a través de los censos.

Para el efecto, en la primera parte del documento se hará énfasis en la relación existente entre el dato personal, la información, el gobierno electrónico y los censos de población y vivienda. En la segunda, se precisarán algunos aspectos del "*data protection*" y se analizarán los riesgos que involucra el tratamiento indebido de datos personales. En la última parte se abordará el estudio del tratamiento de datos para fines estadísticos y las implicaciones de la reserva estadística desde la perspectiva del derecho nacional e internacional. Finalmente se presentarán las principales conclusiones. Se espera que los elementos involucrados en este documento contribuyan a la formulación de algunas sugerencias que deberían considerarse no sólo al momento de implementar el censo sino cuando se utilicen los datos recolectados con ocasión del mismo.

2 - información y dato personal

Información alude a muchas cosas: libertad, democracia, conocimiento, sociedad y poder. Su circulación y acceso son presupuestos fundamentales de una sociedad moderna y democrática. Por eso, éstos se catalogan como derechos fundamentales[2] . Los datos personales[3] , por su parte, son una especie de información que por su naturaleza y por referirse al ser humano adquiere connotaciones especiales que los hacen merecedores de un tratamiento legal particular con miras a evitar la vulneración de derechos fundamentales y las libertades individuales a partir del tratamiento inadecuado de datos personales. Suministrar, recolectar y circular información personal se ha convertido en una actividad cotidiana de las personas y de las entidades públicas y privadas. Cuando alguien busca empleo, desea pagar

2 Refiriéndose al carácter fundamental de la circulación y acceso a la información así como a su uso e incidencia en la sociedad, la Corte Constitucional colombiana ha señalado que "*La sociedad se construye a partir de información que se transmite. Conceptos como poder y vida están estrechamente ligados a la información. (…). En este orden de ideas, puede afirmarse que la existencia misma de la sociedad y fenómenos sociales –constitucionalmente relevantes- como la familia y la personalidad, dependen de la información (…). Resulta innegable que la protección a la circulación y el acceso a la información reúne las condiciones para que sea considerado un derecho fundamental*" (Cfr. Corte Constitucional, sentencia T-227 del 17 de marzo de 2003. M.P. Dr. Eduardo Montealegre Lynett).

3 El dato personal hace relación a cualquier información sobre una persona

sus impuestos o pretende adquirir un bien o servicio, por ejemplo, debe proporcionar algunos datos personales a un tercero. Paralelamente, las empresas y entidades del sector público solicitan información personal para adoptar decisiones o prestar un servicio

La información y los datos personales son bienes constitucionalmente protegidos. El artículo 20 de la Carta establece la garantía a toda persona para "*informar y recibir información veraz e imparcial*". De esta manera, el derecho al acceso y a la difusión de la información es consistente con la Constitución siempre y cuando reúna las citadas dos condiciones: veracidad e imparcialidad.

La gama de informaciones que se puede producir acerca de una persona es diversa. Ella puede estar relacionada con: transacciones financieras, consumo de estupefacientes, solvencia económica, creencias religiosas, la salud, los procesos y condenas criminales, nuestra raza, profesión, los títulos y grados académicos, el comportamiento sexual, las aficiones, los salarios, nuestras ideas políticas, nuestra familia, etc. Cualquiera de estos datos puede ser la base de una decisión que afecta, directa o indirectamente, positiva o negativamente, a la persona. De esta manera, en el contexto de la sociedad de la información, se ha convertido rutinario "catalogar" o "calificar" al ser humano por lo que se pueda concluir respecto de sus datos personales incluidos en bases de datos. En otras palabras, la persona es y será lo que se interprete de su información personal.

El tratamiento de miles de millones de datos personales puede obedecer a diversos fines lícitos o ilícitos: Seguridad nacional, tributarios, penales, comerciales, financieros, clínicos, laborales, estadísticos, encuestas, seguridad social, científicos, académicos, sociales, servicios públicos, delictivos (secuestros, extorsiones), y para la realización de negocios, etc. Frente a esta realidad, existe preocupación no sólo por el uso ilegítimo de la información (ya sea para fines no autorizados por el titular del dato o no permitidos por la ley o para realizar actividades delictivas) sino por la eventual negligencia o el abuso en que puedan incurrir los administradores de los bancos de datos o quien tenga poder de decisión sobre los mismos. Una gestión o tratamiento negligente, ilegal o antiético de la información sobre las personas puede traducirse en una violación de sus derechos fundamentales[4].

3 - Gobierno electrónico, datos personales y censos de población y vivienda

El uso eficiente y responsable de las tecnologías de la información en la gestión pública es un imperativo en un Estado moderno. La correcta aplicación de la

4 De conformidad con la doctrina, el tratamiento automatizado de datos personales puede utilizarse de distintas formas para lesionar los derechos y cercenar las libertades, a saber:

amalgama tecnología-gestión pública beneficiará tanto a los gobiernos como a los ciudadanos. Como se ha puesto de presente, el gobierno electrónico se traduce en un compromiso permanente *"...para mejorar la relación entre los ciudadanos y la administración pública, mediante el intercambio eficaz y eficiente de servicios, información y conocimiento."*[5] Para María Clara Gutiérrez[6] , "*el gobierno electrónico es mucho más que poner en marcha el gobierno on-line: es la instancia en que los gobiernos son interactivos, interjurisdiccionales, totalmente conectados con los ciudadanos trabajando conjuntamente en los temas y encontrando soluciones a políticas y programas de manera coherente y democrática.*"[7] . Expertos destacan el rol de la información en la gestión pública al afirmar que "*El gobierno electrónico es un gobierno inteligente. Está organizado alrededor de la gestión y utilización de la información. El gobierno inteligente es esencial en una sociedad donde la información se ha convertido en una pieza esencial.*"[8] (Subrayo)

Los sistemas de información son el eje del funcionamiento de un Estado moderno y del denominado "*e-government*". Un sistema de información confiable, completo y bien administrado en cabeza de la administración pública facilitaría su gestión, lo cual redundaría en beneficio de los administrados. Este, por ejemplo, le permitiría al Estado: (i) Prestar servicios de manera mas sencilla (simplificación de trámites), rápida y económica; (ii) maximizar el uso de la información que reposa en las entidades públicas sin que sea necesario estar recurriendo permanentemente al ciudadano para que suministre información que éstas poseen (iii) diseñar políticas públicas más eficientes; (iv) planear, organizar y controlar las operaciones relacionadas con la gestión tributaria, aduanera, cambiaria y otras; (v) mejorar los servicios de salud, seguridad nacional, inteligencia militar e investigaciones penales, disciplinarias, etc.

---

tomando decisiones que afecten negativamente a los sujetos sin que ellos tengan conocimiento de por qué se resuelve de esa manera; elaborando perfiles incorrectos de las personas o un perfil de los individuos que permita un eficaz control sobre sus actividades; haciendo una simulación de las reacciones o comportamientos futuros de los individuos, fundamentándose para ello en sus datos; actuando negligentemente, no actualizando, borrando o complementando los datos registrados, etc. (Velásquez Bautista, Rafael. Protección jurídica de datos personales automatizados. Editorial Colex. Pág. 31. Madrid. 1993)

5 Afirmación de la División de Economía y Administración Pública de Naciones Unidas. http://www.unpan.org/egovernment2.asp. Citado por María Clara Gutiérrez

6 Gutiérrez Gómez, María Clara. Hacia el gobierno electrónico: elementos para el desarrollo de una política estatal. Artículo publicado en el libro "Derecho de Internet & Telecomunicaciones" del "Grupos de Estudios en Internet, Comercio Electrónico y Telecomunicaciones (GECTI)" de la Facultad de Derecho de la Universidad de los Andes. Bogotá, Legis, noviembre de 2003.

7 *Towards a Government for the Knowledge Age: Regional Perspective.* Privacy Council Office of Canadá, Mayo 2002. Citado por María Clara Gutiérrez.

8 ALCOCK, R.Y LENIHAN, D. Changing Government. Volumen 2: Results of the Crossing Boundaries. Cross-Country Tour. Enero 2001

En prácticamente todos los países del mundo tanto el sector público como el privado han recurrido a la creación y uso de múltiples sistemas de información contentivos de datos personales de los ciudadanos. A título de ejemplo, en Colombia existen numerosas bases de datos[9] en las cuales se puede encontrar, entre otros, millones de datos personales referentes a diversos aspectos de la persona como su identificación e información dactiloscópica, las historias clínicas, los aportes al sistema de seguridad social, la afiliación a medicina prepagada, pensiones, riesgos y salud, impuestos, registro mercantil, hojas de vida, censos, estadísticas, antecedentes penales y disciplinarios, órdenes de captura, sanciones por infracciones de tránsito, registro de proponentes, comportamiento financiero (hábitos de pago), bienes, etc.

Los censos[10] son el principal medio de que dispone el Gobierno para recolectar, procesar y difundir información personal de los ciudadanos. Por eso, los censos de población y vivienda se han considerado como la piedra angular del sistema nacional de información estadística del país: "*Por su cobertura poblacional, temática y territorial, la información censal y sus múltiples aplicaciones constituyen el eje sobre el cual se sustenta todo el proceso de construcción de la información estadística y sus actuales y potenciales usos en la planeación y gestión del desarrollo*"[11].

La realización del censo implica recoger, recopilar, evaluar, analizar y publicar o divulgar datos demográficos, económicos y sociales relativos a todos los habitantes y a todas las viviendas y sus ocupantes en un país. Son muchos los objetivos que justifican la implementación de los mismos[12]. Para el efecto, el próximo censo que se implementará en Colombia implicará el diligenciamiento de un cuestionario a

9 Un estudio sobre las principales bases de datos públicas y privadas existentes en Colombia forma parte del siguiente texto: Remolina Angarita, Nelson. Centrales de información, habeas data y protección de datos personales: Avances, retos y elementos para su regulación. Capítulo de libro publicado en "Derecho de Internet & Telecomunicaciones" (Legis, noviembre de 2003).

10 Censo significa "*el conteo de todas las personas, los hogares y las viviendas de la totalidad del país, en un momento determinado, para conocer las principales características de cada uno de ellos*." www.dane.gov.co

11 www.dane.gov.co

12 Para el caso colombiano, el DANE cita los siguientes: (i) Obtener información que sea actualizada, oportuna y confiable sobre la población total del país, su distribución espacial, a nivel de regiones, departamentos, municipios y localidades, así como sus características demográficas básicas. (ii) Generar información básica actualizada sobre las condiciones económicas, sociales y culturales de la población para apoyar de manera eficiente la formulación de planes y la ejecución de políticas de desarrollo socioeconómico en todos los niveles territoriales del país; (iii) Permitir el cálculo del monto de la transferencia desde el gobierno central hasta los departamentos, municipios y localidades, estableciendo el volumen de votaciones; (iv) Determinar las características de los hogares, saber cómo es su conformación y las condiciones que viven sus integrantes y (v) Averiguar las condiciones en que se encuentran las viviendas y establecer con qué servicios básicos cuentan (www.dane.gov.co)

través del cual se recolectará diversa información sobre todas y cada una de las personas, hogares y viviendas. El Departamento Administrativo Nacional de Estadísticas (DANE) es la entidad encargada de la planeación, recolección, procesamiento, evaluación y difusión de la información censal.

Según el DANE el censo no sólo consiste en enumerar el total de personas, hogares y viviendas sino que el mismo permitirá conocer: *"(•) Cuáles son las condiciones económicas, sociales y culturales de la población y sus características en cuanto a sexo, edad, pertenencia étnica, estado civil, nivel educativo, migración, ocupación y fecundidad.(•) Las características de la vivienda en cuanto a calidad de materiales, condiciones higiénicas y los servicios con que cuenta, y (•) La forma de tenencia de la vivienda por parte del hogar, las necesidades de las personas que conforman el hogar, su nivel de hacinamiento y su calidad de vida*".

Respecto de los millones de datos personales que se recolectarán surgen algunas inquietudes: ¿Qué datos específicos sobre cada persona y vivienda se recolectarán? ¿Quién define qué datos se recolectarán? ¿Cuál es el criterio para definir los datos que se recolectarán a través de las encuestas? ¿Estos datos guardan directa relación con la finalidad del censo? ¿Son dichos datos los estrictamente necesarios para alcanzar los cometidos del censo? ¿Para qué se utilizará toda esa información? ¿la información censal es pública o reservada? ¿Existe alguna limitación respecto del uso de dicha información? ¿La información del censo será únicamente utilizada o procesada por el DANE o éste la circulará a otras entidades? ¿Puede el DANE transmitir dicha información a entidades privadas? ¿Se puede remitir la información del censo a entidades internacionales o dependencias de gobiernos extranjeros? ¿Puede una persona negarse a proporcionar su información? ¿Existen sanciones legales por el uso inadecuado de la información recolectada en los censos? ¿Cómo se garantiza la seguridad de la información censal de manera que no se accedida por personas no autorizadas? ¿Los actuales sistemas de seguridad son realmente seguros? ¿Cómo se evitará la incorporación de datos erróneos, falsos o incompletos? ¿Los datos recolectados se archivará de manera indefinida o su tratamiento será temporal? ¿Cómo evitar que los datos del censo no se utilicen para fines no autorizados por la ley? ¿Quién garantiza a los ciudadanos que sus datos serán tratados de manera leal y lícita? ¿Los datos del censo serán interconectados con otra información que reposan en entidades públicas diferentes del DANE –por ejemplo datos tributarios, penales, de salud, entre otros-?, y ¿Quién certifica o controla que el DANE trate adecuadamente los datos personales de los colombianos?

Como veremos más adelante, algunos de estos interrogantes tienen respuesta en la legislación y jurisprudencia. Otros representan un reto sobre el cual no existe absoluta garantía de su cumplimiento. Casos como el de Choice Point[13] , por ejemplo,

[13] *ChoicePoint Online (www.choicepointonline.com)* es una compañía que ofrece el servicio de acceder rápidamente, vía internet, a más de 14 billones de datos. El 13 de abril de 2003 se publicó en la página web de la CNN en español un artículo titulado "*Programa secreto de*

han puesto de presente que en materia de tratamiento de datos no hay sistemas seguros y que realizar cualquier negocio con datos personales es una tentación a la cual no se resisten algunas personas. A las normas no sólo se les escapan los impredecibles efectos de las modernas tecnologías que se ofrecen en el mercado sino el comportamiento humano frente al uso de las tecnologías y de los datos personales. En síntesis, dicho caso y otros que destacaremos más adelante constituyen precedentes que proporcionan al ciudadano fundadas razones para desconfiar de lo que sucede con sus datos personales administrados por entidades públicas y privadas.

4 -Retos del gobierno electrónico

La gestión estatal no es incompatible con la protección de los datos personales. De hecho, el tratamiento leal y lícito de la información de las personas constituye un deber imperativo en cabeza de los administradores de bancos de datos de naturaleza pública[14] y privada. Este debe ser un reto y una obligación que se debe superar en el contexto del gobierno electrónico. Para empezar, es fundamental crear una cultura de protección de los datos personales de los ciudadanos por parte de los funcionarios que tienen acceso a ellos.

Si bien la información juega un rol esencial en la gestión gubernamental, existen limitaciones para maximizar el uso de la misma en el cumplimiento de los cometidos estatales. Razones de índole económica, tecnológica, organizacional, cultural y de seguridad pueden ser las causantes de esta situación. A título enunciativo veamos algunas de ellas: (i) Insuficiencia de recursos para contar con una infraestructura tecnológica apropiada y para mantenerla a tono con los avances tecnológicos;

EE.UU tiene fichados a millones de latinoamericanos". Allí se puso de presente que dicha empresa adquirió los siguientes datos personales de más de 31 millones de colombianos: *datos de identificación de ciudadanos de todo el país, incluyendo la fecha y lugar de nacimiento de cada habitante, su número de pasaporte y de identificación nacional, su familia y su descripción física*" Recientemente, un periódico colombiano afirmó que "*por esta información y las de muchos otros países en la región, la compañía recibió tan sólo el año pasado más de 11 millones de dólares*" (Periodico el Tiempo. Págs 1-2 del lunes 12 de mayo de 2003)

Según la CNN, *"ChoicePoint dice que compra los archivos de subcontratistas radicados en México, Colombia, Venezuela, Costa Rica, Guatemala, Honduras, El Salvador y Nicaragua" De Brasil, Choicepoint vende números telefónicos y detalles sobre líderes empresariales". (…) "En México, ChoicePoint dice que compra los registros de licencias de conducción de seis millones de habitantes de la ciudad de México y el padrón electoral de todo el país, entregándolos al gobierno de Estados Unidos".*

14 Sobre el particular, la Corte Constitucional ha precisado lo siguiente: "*La protección al derecho al habeas data en todas sus expresiones es una obligación del Estado que debe cumplirse de manera efectiva, sin dilaciones injustificadas, pues como se ha podido determinar, además de ser de naturaleza fundamental, constituye una garantía de protección para otros derechos fundamentales como la libertad, debido proceso, buen nombre, la honra e intimidad, así como del respeto por el principio de la dignidad humana"* (Sentencia T-310 de 2003)

(ii) Ausencia de una política integral, coherente, coordinada y de largo plazo sobre el uso de los sistemas de información en la gestión estatal; (iii) Falta de voluntad y compromiso político para implementar, mantener y mejorar los sistemas de información; (iv) Desconocimiento por parte de algunos funcionarios públicos sobre el manejo adecuado de la tecnología en sus gestión (brecha cultural) y por ende la existencia de cierta reluctancia respecto del uso de la misma; (v) Temor de algunos funcionarios públicos por el efecto que puede generar la adecuada implementación de las tecnologías de información en la gestión pública respecto de la pérdida de puestos de trabajo (reemplazo de la máquina por el ser humano); (vi) Falta de definición integral sobre las características mínimas de la tecnología adecuada para la gestión estatal de manera que ésta no sea incompatible con las tecnologías adquiridas o desarrolladas por las diferentes entidades (incompatiblidad tecnológica intergubernamental) o se convierta en obsoleta o rezagada rápidamente ¿La tecnología de hoy será compatible y suficiente con la que se desarrollará en el mediano y largo plazo? ¿La información que hoy archivamos electrónicamente se podrá recuperar y utilizar con los sistemas tecnológicos del mañana?; (vii) Vulnerabilidad de las redes informáticas frente a riesgos de seguridad (pérdida de información, virus, accesos no autorizados a sistemas de información, daños a la infraestructura tecnológicas, etc.); (viii) Desconfianza de parte de la ciudadanía respecto de la gestión pública tecnológica. En medio de una etapa de transición entre un mundo no tecnológico a uno tecnológico la brecha cultural y educativa son dos aspectos fundamentales a considerar y superar, y (ix) Falta de de tratamiento integral de la información en el sector público porque ésta se encuentra dispersa, repetida y desactualizada: "*para que el gobierno electrónico tenga resultados exitosos y satisfactorios es indispensable (…) que las entidades que lo conforman (…) cuenten con información oportuna y relevante para intercambiar entre sí*"[15].

El eficaz cumplimiento de las funciones constitucionales y legales del Gobierno requiere, entre otras, contar con fundamentos jurídicos que permitan bajo ciertas condiciones la interconexión de la información que reposan en las diferentes entidades estatales sin que se lesionen o amenacen vulnerar los derechos fundamentales de las personas. Esta integración de la información implica unir e interconectar las diferentes fuentes de información dispersa que actualmente existe.

En otras palabras, es importante que el Gobierno pueda utilizar bajo ciertas condiciones la información incorporada en las bases de datos (manuales o sistematizadas) de las entidades públicas y privadas. No obstante, el tratamiento leal, lícito, transparente y ético de datos personales constituye una garantía de la persona que debe ser respetada en la gestión gubernamental. La obtención y uso de información personal para alcanzar cometidos estatales debe ir acompañada del respeto de los derechos de las personas en cuanto al tratamiento de sus datos

15 Gutiérrez, María Clara. Ob. Cit.

personales. Todo lo anterior no sólo permitirá generar confianza en los ciudadanos respecto del uso de sus datos sino que es una obligación en cabeza del administrador y del usuario de la información el respetar los postulados legales y éticos del tratamiento de datos personales. Por eso, el Gobierno no sólo deber ser garante de los derechos fundamentales de los ciudadanos frente a sus datos personales sino respetuoso de las normas que confieren tratamientos especiales a ciertos tipos de información, las cuales exigen, entre otros, garantizar la reserva o confidencialidad de determinada información y no utilizarla para fines diversos a los permitidos por la ley.

Lo anterior es una constante que se vislumbra en regulaciones sobre el gobierno electrónico. En los Estados Unidos, por ejemplo, la *E-Government Act* de 2002, entre otros, promociona la colaboración entre entidades gubernamentales con miras a proveer mejores servicios e información al ciudadano así como ofrecer mayores herramientas informacionales al gobierno para la adopción de sus políticas. Indica la norma que lo anterior debe realizarse dentro de un marco que respete las leyes sobre protección de la privacidad y seguridad nacional entre otras. La sección 208 (*Privacy provisions*), por ejemplo, tiene como propósito obligar a las entidades gubernamentales a adoptar políticas para proteger la privacidad y la información personal de los ciudadanos en el desarrollo de un sistema centralizado de información para el funcionamiento eficiente del gobierno electrónico.

5- Precisiones sobre el régimen de proteccción de datos personales.

La protección de los derechos humanos frente al uso inapropiado de los avances tecnológicos de información, así como el conflicto entre la libertad de información y el derecho a la privacidad[16] son dos temas latentes de nuestro tiempo que aún no han sido solucionados satisfactoriamente. No es raro ver como en el mercado cada día se introducen sofisticadas tecnologías de información cuyo uso inadecuado, aunque no se perciba fácilmente, crea inimaginables e imperceptibles conductas que pueden comprometer negativamente la protección de los derechos humanos o libertades individuales. *Privacy Internacional* ha destacado que, por ejemplo, las nuevas tecnologías de información están significativamente aumentando caminos tendientes a erosionar el derecho a la intimidad de las personas[17] . Reconocidos autores en la materia, por su parte, coinciden en afirmar que las preocupaciones sobre la protección del

16Privacidad e intensidad son conceptos diferentes. El primero es el género y el segundo la especie.Todo dato íntimo es privado pero no todo dato privado pertenece a la esfera íntima de las personas.

17 Privacy International. Privacy and Human Rights 1999:An international survey of privacy laws and developments. Londres y Washington, 1999.

derecho a la intimidad y la privacidad en general, son más grandes ahora que en otro momento de la historia reciente[18].

"*La información lo es todo*". Los datos sobre las personas así como el uso de bases de datos son "insumos" fundamentales para casi todas las actividades públicas y privadas. Hoy en día, el Estado y los particulares quieren tener información de las personas para tomar e implementar decisiones de diversa naturaleza (económica, seguridad nacional, social, política, laboral, profesional, académica, financiera, comercial, etc.)

El tratamiento de datos personales es una realidad de la sociedad de la información y no tiene marcha atrás. Frente a esta situación, las leyes de protección de datos no buscan impedir el uso de los mismos. No. Ellas buscan que el tratamiento de datos personales esté rodeado de garantías encaminadas a evitar abusos o conductas indebidas que se traducen en amenazas o vulneraciones de los derechos fundamentales de la persona. Se quiere, en últimas, exigir al administrador o responsable del tratamiento de datos personales que cumpla su tarea ética y legalmente. Si éste cumple su rol correctamente pues no se verán vulnerados ni amenazados los derechos de las personas cuyos datos son incorporados diariamente en bases de datos y circulados a través de las mismas a nivel local e internacional.

La Constitución colombiana, por ejemplo, consagra límites en cuanto al acceso, circulación y el tratamiento de la información personal. El inciso segundo del artículo 15 ordena que "*en la recolección, tratamiento, y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución*". Así, el derecho a la intimidad protege a las personas del acceso a datos personales que de manera aislada o en conjunto permiten conocer aspectos de la vida privada o familiar de las personas. El derecho al buen nombre supone que no debe circular información falsa, errónea, incompleta o desactualizada sobre las personas. El debido proceso exige que el tratamiento de datos personales se realice de manera leal y lícita observando el cumplimiento de ciertos mandatos legales, constitucionales o jurisprudenciales. La libertad personal reclama, entre otras, que la persona no sea detenida o "controlada" con fundamento en información errónea. La igualdad demanda, por ejemplo, evitar actos discriminatorios con base en el uso de información sobre las personas.

Con el término ***data protection*** se designa el conjunto de normas y principios que regulan el tratamiento de datos personales en todas sus etapas (recolección, almacenamiento, circulación, publicación y transferencia nacional e internacional). Según Millard y Ford, "data protection" hace alusión a la manera como la información de las personas es recolectada, almacenada, procesada, utilizada,

18 Davies, Simon. "*Re-engineering the right to privacy: how has been transformed from a right to a commodity*". Artículo publicado en: Agree and Rotenberg ed. Technology and privacy: The new landscape. Cambridge: MIT Press, 1997.

divulgada y transferida[19] . El ***habeas data***[20] , por su parte, es una parte importante dentro del campo de acción del "data protection" que ha sido incorporada en muchas constituciones[21] y normas de los países. Representa un derecho fundamental y una herramienta jurídica del ciudadano para que se proteja frente al tratamiento indebido o ilegal que reciban sus datos personales por parte de los administradores de bancos de datos o de archivos de entidades públicas y privadas. El habeas data no se creó para proteger los intereses de los administradores de bancos de datos o archivos sino para exigirle a los mismos que en el tratamiento de datos personales observen una serie de pautas éticas y legales encaminadas a evitar que durante la incorporación, circulación o cualquier uso de los datos personales, no se amenacen o lesionen los derechos fundamentales de las personas a quienes pertenecen o se refieren los datos personales.

Esta última exigencia cobra mucha importancia si se tiene en cuenta que los administradores realizan su labor de manera sigilosa y secreta. Nadie los vigila ni controla. A nadie le entregan cuentas. En fín, el ciudadano cuando entrega sus datos a un administrador realiza un "acto de fé" con la esperanza que su información sea tratada leal, lícita y éticamente por parte de terceros. Adicionalmente, al ciudadano le es prácticamente imposible saber qué se ha hecho o qué se está haciendo con sus datos.

El habeas data propende por el tratamiento adecuado de los datos de las personas. Aunque frecuentemente se ha ligado al derecho a la intimidad, su campo de acción es mucho más amplio ya que a través del mismo también se protegen otros derechos como el buen nombre, la información, la libertad, el honor y la honra. La Carta de Derechos Humanos de la Unión Europea de 2000, busca "*reforzar la protección de los derechos fundamentales, dotándolos de mayor presencia, a tenor de la*

19 Millard, Christopher y Ford, Mark. Data protection Laws of the world. Sweet & Maxwell. Londres. 1999.

20 Para mayor detalle sobre este tema, se sugiere consultar el siguiente texto: Remolina Angarita, Nelson: Data protection: Panorama nacional e internacional. Capítulo de libro publicado en "Internet, Comercio Electrónico & Telecomunicaciones" (Legis, junio de 2002)

21 En Colombia, por ejemplo, este fue consagrado en el artículo 15 de la Constitución a saber: *«Todas las personas (...), 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."*

Dado que mediante la informática y otros avances tecnológicos se facilita la recolección, clasificación, almacenamiento y circulación de datos referentes a todos los aspectos de la vida de las personas, el constituyente colombiano de 1991, ha dispuesto en el segundo inciso del artículo citado que: *«En la recolección, tratamiento y circulación de datos se respetarán la libertad y las demás garantías consagradas en la Constitución»* Este inciso, según la Corte Constitucional,"*define el contexto normativo y axiológico dentro del cual debe moverse, integralmente, el proceso informático. Según este marco general, existen unas reglas generales que deben ser respetadas para poder afirmar que el proceso de acopio, uso y difusión de datos personales sea constitucionalmente legítimo. Las mencionadas reglas se derivan de la aplicación directa de las normas constitucionales al proceso informático*" (Corte Constitucional, Sentencia T-307 de 1999).

evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos"[22] (destaco). Por eso, se introdujo en el artículo 8 de dicho documento la protección de datos personales como un derecho autónomo e independiente del derecho a la intimidad para proteger al ciudadano frente al tratamiento de sus datos personales bajo el contexto de la sociedad de la información[23].

Finalmente, debe anotarse que desde la década de los sesenta organismos internacionales como la ONU, la OECD, el Parlamento Europeo y otros[24], han expedido principios y reglamentaciones relacionadas con el habeas data y el data protection[25]. Muchos de ellos están incorporados en leyes sobre la materia alrededor del mundo[26] y han sido desarrollados jurisprudencialmente por los Jueces, como es el caso de la Corte Constitucional. Aunque existen diferencias entre unos y otros, dado que poseen ámbitos de aplicación diferentes y grados de obligatoriedad

22 Cfr. Considerando No. 4 del preámbulo de la Carta

23 *"Artículo 8. Protección de datos de carácter personal: Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal, para fines determinados y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. El respeto de estas normas quedará sujeto al control de una autoridad independiente"*

24 Sobre el panorama internacional de protección de datos se puede consultar el siguiente texto del autor: Data protection: Panorama nacional e internacional. Capítulo de libro publicado en la obra "Internet, Comercio Electrónico & Telecomunicaciones" (Legis, junio de 2002).

25 (i) Resolución 509 de 1968 de la Asamblea del Consejo de Europa sobre "los derechos humanos y los nuevos logros científicos"; (ii) Resolución 3384 del 10 de noviembre de 1975 de la Asamblea General de la ONU: "Declaración sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad"; (iii) Guía para la protección de la privacidad y transferencia del flujos de información personal elaborada por la Organización para la Cooperación y el Desarrollo Económico (OECD) el 23 de noviembre de 1980; (iv) Convención No. 108 del Consejo de Europa para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal. Suscrita en Estrasburgo el 28 de enero de 1981; (v) Resolución 45/95 del 14 de diciembre de 1990 de la Asamblea General de la ONU: "Principios rectores para la reglamentación de ficheros de datos personales"; (vi) Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; (vii) International Safe Harbor Privacy Principles sucrito el 21 de julio de 2000 por el Departamento de Comercio de Estados Unidos; (viii) Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones electrónicas; y (ix) Carta de Derechos Humanos de la Unión Europea del 7 de diciembre de 2000

26 Por ejemplo: Austria, Bélgica, Dinamarca, Finlandia, Francia, Alemania, Grecia, Italia, Luxemburgo, Portugal, España, Suecia, Reino Unido, Argentina, Chile, Canadá, entre otros.

distintos, los documentos coinciden en señalar una serie de pautas que abogan porque los datos personales sean: "*a) tratados de manera leal y lícita; b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; (...) c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente; d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados; e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. (...)*"[27]

6 - Riesgos que implica el tratamiento inadecuado de datos personales

La peligrosidad del uso indebido de las tecnologías de la información para algunos derechos humanos se pone de manifiesto a través de las siguientes circunstancias:

(a) La publicación de datos que por su naturaleza pertenecen a la esfera íntima de la persona o que pueden ser tomados como elementos para prácticas discriminatorias:

No es fácil determinar a priori la información que pertenece o no a la vida privada de las persona. Los datos que pueden ser considerados como parte de la vida privada para unas personas no lo son para otras[28] . Esto depende de factores culturales, religiosos, políticos y económicos, entre otros. No obstante se puede afirmar que existen "consensos" sobre la naturaleza de cierta información. El comportamiento sexual de la persona, su ideología política o religiosa, entre otros, se catalogan como datos "íntimos" cuyo uso ilegal o desautorizado constituye una violación del derecho a la intimidad.

Este tipo de información también puede convertirse en un factor determinante de decisiones discriminatorias sobre las mismas. Así por ejemplo, una entidad pública que, aunque no lo explicite públicamente, internamente decide no contratar

En http://europa.eu.int/comm/internal_market/privacy/law/implementation_en.htm se puede consultar un informe sobre el estado de implementación de la Directiva 95/46/CE en Europa.

27 Cfr. Art. 6 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 deoctubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (Diario Oficial n° L 281 de 23/11/1995 P. 0031 – 0050)

28 En este sentido ver: Wacks, Raymond. Personal information: privacy and the law. Oxford: Clarendon Press, 1989.

personas en razón a su filiación política y para el efecto consulta algunas bases de datos que han llegado a sus manos. Sobre ésto, el ciudadano afectado seguramente nunca sabrá cuál fue el verdadero motivo de no considerarlo apto para el cargo. En el sector privado, por ejemplo, puede darse situaciones en las cuales descalifican a una persona debido a que pertenece o es simpatizante de determinados grupos religiosos. Aunque siempre existirán explicaciones para motivar estas decisiones, lo cierto es que la persona es quien, en últimas, se ve afectada por el uso indebido o la lectura equivocada de sus datos personales.

La información personal referente al origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos así como la referida a la salud o a la sexualidad han sido consideradas local e internacionalmente como "información sensible"[29] que hace parte de la vida privada de las personas[30]. El uso inadecuado de este tipo de información ha producido catastróficos ejemplos en nuestra historia. Por eso, actualmente el tratamiento de este tipo de información es restringido debido a las consecuencias nefastas que puede ocasionar su utilización indebida[31].

Un caso doloroso de la historia nos ha enseñado que la amalgama compuesta por el uso indebido de la tecnología y el tratamiento ilegítimo de datos personales contribuyó al exterminio de mas de seis millones de personas. En su libro "*IBM y el Holocausto: La alianza estratégica entre la Alemania Nazi y la corporación mas poderosa de América*"[32] Edwin Black sostiene que IBM mediante sus máquinas para tarjetas perforadas dotó al III Reich de capacidad para identificar a Judíos, homosexuales, gitanos[33], izquierdistas y no arios, para confiscar sus propiedades, desplazarlos hacia los ghettos y campos de concentración y finalmente exterminarlos.

---

29 La Corte Constitucional ha manifestado que todo dato se debe recolectar para una finalidad constitucionalmente legítima, lo cual significa, entre otras, "*que no puede recolectarse información sobre datos "sensibles" como, por ejemplo, la orientación sexual de las personas, su filiación política o su credo religioso, cuando ello, directa o indirectamente, pueda conducir a una política de discriminación o marginación*". (Sentencia T-307/99)

30 En este sentido ver la sección 2 de la UK Data Protection Act 1998.

31 En este sentido ver el artículo 8 de la Directiva 95/46 y los "*Safe Harbor Privacy Principles*".

32 Algunos autores que se han referido a este tema son: (1) Bardini, Roberto. Tecnología de avanzada para organizar la masacre IBM y Hitler: una alianza estratégica. Artículo publicado el 11 de octubre de 2003 por Argenpress.info; (2) Traynor, Ian. Gypsies win right to sue IBM over role in Holocaust. Artículo publicado el 23 de junio de 2004 en el período The Guardian. http://www.guardian.co.uk/secondworldwar/story/0,14058,1245284,00.html; (3) Litvinoff, Edgardo. Soluciones para el genocidio: las víctimas del genocidio fueron identificadas con tarjetas fabricadas por IBM. Artículo publicado en: http://www.intervoz.com.ar/2001/0512/suplementos/cultura/nota31821_1.htm

33 Sobre este hecho, una Corte de Apelación Suiza, por su parte, decretó que IBM pudo haber ayudado a Hitler al "*asesinato en masa de manera más rápida y eficiente de lo que hubiere sido posible sin su colaboración*". Cfr. Traynor, Ian. Gypsies win right to sue IBM over role in Holocaust. Artículo publicado el 23 de junio de 2004 en el periódico The Guardian. http://www.guardian.co.uk/secondworldwar/story/0,14058,1245284,00.html

Una filial de IBM en Alemania denominada Deutsche Hollerith Maschinen Gesellschaft (Dehomag) diseñó una maquina "Hollerith"[34] que permitió clasificar unas tarjetas perforadas que contenía datos personales obtenidos en los censos alemanes de 1933 y 1939 para cuya realización se utilizó tecnología IBM. En dicho censo se recolectaron datos que comprendían desde los rasgos étnicos hasta los bienes de las personas. Esta información se incorporó en tarjetas perforadas que luego fueron procesadas en las máquinas clasificadoras permitiendo la creación de perfiles sobre las personas. A partir de éstos, los nazis identificaron a los ciudadanos teniendo en cuenta su aspecto étnico, nacional o económico.

En otras palabras, el uso indebido de la tecnología fue determinante a la hora de manipular rápidamente muchos datos para identificar, localizar, expropiar, deportar y exterminar a millones de personas. Comenta un autor que gracias a dicha tecnología se pudo:

> "*cruzar nombres, direcciones, genealogías y cuentas bancarias de ciudadanos caídos en desgracia. Con las tarjetas perforadas Hollerith adaptadas a sus necesidades, los nazis automatizaron datos sobre judíos, gitanos, izquierdistas, clérigos e 'inadaptados'. Después de identificarlos se podía organizar metódicamente confiscaciones de bienes, deportaciones, reclusión en ghettos o campos de concentración, explotación laboral y, finalmente, la aniquilación masiva*" .
>
> *" Ese mismo sistema, explica Edwin Black, servía para clasificar a las víctimas en los campos de concentración. Cada persona que ingresaba a los centros de reclusión recibía un número de identificación Hollerith. Las tarjetas diseñadas por Dehomag medían 13 centímetros de largo por ocho de alto y estaban divididas en columnas numeradas y perforadas en hileras. Cada prisionero de los campos tenía una ficha. Se identificaban 16 categorías de reclusos. La clave de los homosexuales era el número tres, a los judíos les correspondía el número ocho, a los 'antisociales' el nueve y a los gitanos el 12. Black sostiene que las tarjetas -cuyo propósito inicial fue sistematizar la recolección de información para los censos de población- eran 'un código de barras del siglo XIX para seres humanos*" [35]

(b) La publicación de información errónea, inexacta, incompleta, desactualizada y parcializada.

Esta situación compromete el buen nombre, la honra, el honor y hasta la libertad de las personas. Catalogar a alguien como deudor moroso sin realmente serlo, por ejemplo, no sólo significa que para esta persona prácticamente se le cerrarán las puertas del sistema financiero sino que su buen nombre se ha desvanecido injustamente. Adicionalmente, la realidad muestra que se constituirá en carga del ciudadano el tratar de "limpiar" su buen nombre que se ensucio por la negligencia de quien suministró información errónea sobre el mismo o por parte de quien "ciegamen-

34 Máquina clasificadora de tarjetas Hollerich

35 Cfr. Bardini *op cit.*

te" únicamente se interesó en incorporar en su base de datos información sin realizar sobre la misma ningún control de calidad. Mientras la fuente de información y el banco de datos tratan mutuamente de liberarse de responsabilidades, el ciudadano padece los efectos negativos de la situación.

La Corte ha condenado y rechazado la conducta negligente de algunos administradores de datos colombianos que no obran con el cuidado y diligencia que impone la responsabilidad propia de sus actividades[36] . Por ejemplo, se ha descalificado la conducta de administradores que han admitido y registrado datos suministrados por particulares respecto de otros sin verificar si había sido judicialmente definido el conflicto entre las partes, haciéndose responsable también por el daño al buen nombre de la persona afectada *: "Admitir como válida la conducta que en el asunto examinado observó la central de datos implicaría extender hacia el futuro y sin ninguna clase de control las posibilidades de que cualquiera pudiese suministrar a esta clase de empresas, con su beneplácito, datos sin confirmar, tergiversados, manipulados o sencillamente falsos, con el fin de presionar pagos, configurándose así formas extorsivas de cobranza que desconocerían las competencias de los jueces y que, por tanto, de ninguna manera podrían entenderse como sano ejercicio del derecho a la información"*[37] .

Incorporar erróneamente el número del documento de identificación de un ciudadano en una base de datos de un organismo de seguridad o no actualizar las órdenes de captura que rutinariamente se expiden cuando se investiga una conducta punible se traduce en la supresión de la libertad de las personas por algunas horas o días. Un caso estudiado por la Corte Constitucional, demostró, entre otros, los graves perjuicios que puede sufrir una persona por la negligencia de un administrador de un banco de datos en la no eliminación inmediata de datos negativos. La sentencia T-310 del 10 de abril de 2003 trata el tema de órdenes de captura que, a pesar de haber perdido su vigencia, permanecen registradas en las bases de datos o sistemas de información de la Fiscalía y las entidades encargadas de la preservación del orden público y la seguridad ciudadana.

Según los hechos relatados en la sentencia, un ciudadano estuvo vinculado a un proceso de carácter contravencional por lesiones en accidente de tránsito, del cual conoció el Juzgado Segundo Penal Municipal de Medellín. El Juez decretó la terminación del proceso por indemnización integral y el 9 de febrero de 1998, mediante oficio dirigido al Cuerpo Técnico de Investigación (CTI) de la Fiscalía General de la Nación, ordenó la cancelación de orden de captura. Esta instrucción sólo fue cumplida 4 años después.

36 En muchos casos la Corte también ha encontrado que los administradores de bancos de datos han obrado correctamente.

37 Cfr. Corte Constitucional, Sentencia No.T-199/95.

Durante esos cuatro años, el ciudadano figuró "ilegalmente" registrado en la base de datos del DAS con "orden de captura vigente". Por eso, fue privado de la libertad "20 veces aproximadamente". Relata el ciudadano que "*cada retención se ha prolongado por términos que oscilan entre cinco (5) y noventa y dos (92) horas, siendo maltratado física y verbalmente en varias ocasiones*"[38].

(c) La potencialidad de la informática para recopilar y almacenar masivamente datos personales de cualquier naturaleza y la facilidad para acceder a esa información.

Un dato aislado, en principio, no genera mayores riesgos a la persona. Pero varios interconectados si pueden constituirse en un problema. Esta es la razón por la cual existe reticencia al uso de bases de datos como centrales universales.

La interconexión de bases de datos permite la recopilación masiva, instantánea e indiscriminada de datos sobre una persona desde cualquier parte del mundo. En efecto, las bases de datos pueden actuar como una central de registro universal de la información personal o como parte de una red global de la cual se alimentan otras centrales de registro. Lo anterior es así porque es fácil incorporar información personal en bases de datos, y transferirla a terceros u otras bases de datos ubicadas en cualquier parte del mundo. Gracias a la tecnología, toda la información que una persona ha suministrado a diferentes bases de datos en diversas partes del mundo puede ser unida o compilada en una central de información. Como resultado de lo anterior, una persona, en cualquier momento podría tener acceso a un sinnúmero de datos personales sobre un tercero, la cual podría ser utilizada para diversos fines.[39]

En fin, actualmente no es difícil que en cuestión de segundos y con el número de cédula o de pasaporte de una persona, por ejemplo, se obtenga una cantidad masiva e indiscriminada de la información de cualquier persona, que repose en bases de datos o en archivos públicos y privados nacionales o internacionales[40]. La compilación de tanta información sobre la persona así como el eventual acceso a la

38 En dicho caso, la Corte concluyó lo siguiente: (i) El incumplimiento del DAS de mantener actualizados sus registros y archivos, trajo como consecuencia la vulneración del derecho al habeas data y, en su momento, la violación de los derechos fundamentales a la dignidad, libertad, debido proceso, intimidad, buen nombre, honra y trabajo; (ii) "*Es preocupante, que existiendo una normatividad tan completa y coherente en materia de registro de órdenes de captura y su cancelación, sigan sucediendo en el país casos como el presente, en los cuales la negligencia de las entidades administradoras de base de datos y de los despachos judiciales, lleguen hasta el punto de atentar contra la dignidad humana de las personas*".

39 Todo lo anterior sucede sin que la persona a que se refiere la información conozca qué se está haciendo con la misma.

40 Dicha información puede hacer referencia a cualquier aspecto de la persona. Veamos: (i) datos biográficos (nombre, fecha y lugar de nacimiento, domicilio, nacionalidad, raza y sexo, entre otros); (ii) datos sobre el domicilio (dirección, teléfono, barrio, estrato socio económico,

misma por parte de terceros son riesgos latentes que ponen en peligro el derecho a la privacidad de la misma. Así como ha evolucionado y ampliado la concepción de la privacidad, de la misma forma han surgido nuevos mecanismos o conductas que la desconocen. Uno de ellos es, precisamente, es el control ejercido sobre la persona con ocasión de la recolección, comparación (o análisis cruzado), la adición o agregación de los datos, numerosos y minuciosos, que son procesados por medio de computadoras o las tecnologías de información y comunicación (TICS) en general.

(d) La manipulación y/o "cruce" de los datos almacenados que permiten crear perfiles virtuales de las personas (conocer sus pautas de comportamiento, sus tendencias políticas, religiosas, sexuales, entre otras), que pueden resultar valoradas, bien o mal, para las más diversas actividades públicas o privadas.

Esto es una realidad. Como se advirtió en páginas anteriores, la persona es lo digan sus datos personales. Quien necesite saber cualquier cosa sobre alguien simplemente acudirá a consultar bases de datos de diferente índole. Todo lo que se encuentre en las mismas será la imagen ("perfil virtual") que el lector de dicha información se crea sobre la persona. Respecto de la misma información varios lectores pueden sacar conclusiones diferentes e incluso totalmente opuestas. Adicionalmente, es posible que la información que se consultó en las bases de datos no sea de calidad (completa, actualizada, veraz, imparcial). En todas las hipótesis, el principal afectado o beneficiado de la situación será el ciudadano.

El acceso indiscriminado a bases de datos por parte de terceros también puede poner en riesgo los derechos y libertades de las personas. Un caso estudiado por la Corte Constitucional en el que entidades públicas "colgaron" en Internet bases de

entre otros); (iii) datos familiares (estado civil; nombre de padres y hermanos, número y nombre de hijos, entre otros); (iv) datos laborales (nombre del empleador, nombre del jefe, cargo, salario, responsabilidades, dirección, fax, teléfono, dirección electrónica, horario de trabajo, entre otros); (v) información financiera (ingresos, seguros, saldo promedio, número de cuentas de ahorro o corriente; número de tarjetas de crédito, comportamiento financiero, entre otros); (vi) información médica (grupo sanguíneo, enfermedades, alcoholismo, uso de medicamentos, entre otros); (vii) información ideológica (pertenencia a partidos políticos y sindicatos, comportamiento respecto la frecuencia a votar, religión, entre otros); (viii) información académica (colegios y universidades, títulos obtenidos, calificaciones, investigaciones disciplinarias, entre otros); (ix) Información policíaca (infracciones, licencia de conducir, detenciones preventivas, entre otros); (x) Pasatiempos (actividades deportivas, tipos de lectura preferida, programas de televisión, hobbies, lugares visitados en vacaciones, entre otros); (xi) Hábitos (lugares normalmente frecuentados, clase de libros adquiridos, tipo de ropa utilizada, entre otros); (xii) Información sobre viajes y comunicaciones (uso de transporte público, aerolínea o empresa de transporte frecuentemente utilizada, celular, bipper, sitios preferidos para pasar las vacaciones); y (xiii) Información patrimonial (bienes inmuebles y muebles, obligaciones pecuniarias, ubicación de bienes, actividad económica que desarrolla, entre otros)

datos sobre aspectos patrimoniales y de salud de las personas puso de presente que las condiciones de acceso indiscriminado a datos personales, aunque esta sea precaria, constituyen un riesgo cierto que debe ser evitado ante la posible elaboración de perfiles virtuales. En la sentencia, la Corte precisó lo siguiente:

> *"Ante el surgimiento del poder informático, la existencia de un número único de identificación de los nacionales colombianos se ha constituido hoy en un factor de riesgo para el ejercicio de los derechos fundamentales. Esta situación se hace evidente, ante la relativa facilidad de efectuar los llamados «cruces de datos», de tal forma que con la digitación de un sólo dato (el número de identificación) y la disponibilidad de varias bases de datos personales, es posible en contados minutos elaborar un «perfil virtual» de cualquier persona.*
>
> *Esta posibilidad, cercana a la vulneración del derecho a la autodeterminación informática, se pone en evidencia en el caso bajo estudio, aunque de manera aparentemente inocua. En este orden de ideas considera la Sala que, aunque precaria, tanto la información patrimonial, como la información acerca del núcleo familiar y de las características de la afiliación al sistema de seguridad social en salud del señor Carlos Antonio Ruiz Gómez, permite construir una pequeña semblanza del titular, que incluso podría perfeccionarse ante la posibilidad de acceso indiscriminado a nuevas bases de datos personales.*
>
> *Esta situación afecta sus derechos fundamentales, no sólo en lo que concierne a la autodeterminación informática, sino también en lo relativo a su intimidad, libertad e integridad física, entre otros.*
>
> *Considera entonces la Sala que, ante la posibilidad de acceso a múltiples bases de datos personales (publicadas ahora en la Internet), el fortalecimiento del poder informático (caracterizado por su titularidad en ocasiones anónima), y la carencia casi absoluta de controles, se han incrementado los riesgos de vulneración efectiva no sólo del derecho a la autodeterminación informática, sino de los demás derechos fundamentales puestos en juego en el ámbito informático: la intimidad, la libertad e incluso la integridad personal"*[41].

Como se puede observar, es fácil que un tercero obtenga información sobre una persona, sin que la misma lo haya autorizado o se entere de qué está pasando con su información, ni quién la tenga o para qué la esté utilizando: ¿Esta situación pone en peligro los derechos y libertades de las personas?

---

41 La Corte concluyó lo siguiente: *"las condiciones de acceso indiscriminado a la información, aunque esta sea precaria, constituyen un riesgo cierto que debe ser evitado ante la posible elaboración de perfiles virtuales. Esta situación conduce a analizar el alcance del principio de individualidad. Según este principio, el Departamento Administrativo de Catastro, como administrador de datos personales, debe abstenerse de realizar conductas que faciliten el cruce de datos y la construcción de perfiles individuales. Nuevamente encuentra la Corte que, Catastro, con la publicación de información patrimonial del señor Carlos Antonio Ruiz Gómez, al facilitar las condiciones para que la misma sea sumada a otra, con el concurso de diversas fuentes de información, vulnera su derecho a la autodeterminación informática*" (Corte Constitucional, Sentencia T-729 del 5 de septiembre de 2002.)

(e) El riesgo de que la información de las personas sea conocida y manipulada por grupos ilegales para diferentes fines (terrorismo, chantajes, extorsiones, saboteos, discriminaciones, etc.)

Más que un riesgo, estamos frente a una realidad. Un caso de la historia colombiana que ilustra este problema es lo sucedido con alias "Simón Trinidad". En efecto, un exbanquero (Ricardo Ovidio Palmera Pineda, alias *"Simón Trinidad"*) que ingresó a las filas de la guerrilla se llevó consigo información sobre los clientes del Banco del Comercio de Valledupar, la cual utilizó posteriormente para decidir qué personas serían objeto de extorsiones y secuestros con fines económicos: "*Con él se llevó una larga lista de las transacciones realizadas por los millonarios de la región, que después utilizaría para extorsionar y secuestrar a comerciantes y agricultores a nombres de las FARC*"[42], "*no sólo sabía quién era cada quien sino cuánto tenía cada uno*"[43]. Como consecuencia de lo anterior, señala la prensa, muchas familias, entre otras, fueron condenadas al exilio (en algunos casos luego de que la guerrilla les secuestraba algún familiar) y otras entraron en crisis o ruina económica[44].

(f) La utilización de la información para fines no permitidos por la ley o no autorizados por el titular del dato.

La información personal debe ser recolectada para uno o más fines específicos y lícitos. No obstante, la misma puede estar siendo utilizada para propósitos diversos o incompatibles con los autorizados o permitidos por la ley. "*Function creep*" se refiere al fenómeno consistente en dar uso incompatible a la información colectada para un propósito y utilizada para otros no autorizados, ni informados a la persona concerniente. En la práctica, todos estamos seriamente expuestos a este fenómeno. No debe sorprendernos que sin nuestra autorización y conocimiento algunos administradores de bancos de datos utilicen nuestra información personal para fines diversos o incompatibles a los autorizados. Por eso, Jain afirma que "*en cualquier sistema de redes de información es difícil garantizar que la información recolectada se utilizará únicamente para los fines autorizados*"[45]. Tomko, por su parte, destaca que la "*tentación de usos secundarios o no autorizados de la información será muy útil especialmente si el crimen, los fraudes fiscales y el terrorismo aumentan en nuestra sociedad*".

Según Davies, la historia de los sistemas de identificación alrededor del mundo provee evidencia del fenómeno de "*function creep*". Así, el uso del *Social Security*

42 Cfr. Revista Semana. Edición No. 1131. Pág. 22. Bogotá, enero 5-12 de 2004.

43 Cfr. Diario El Tiempo. Pág. 1-3. Artículo titulado *"El Cesar temblaba por un cheque llamado 'Simón'"* Bogotá, enero 11 de 2004.

44 Ídem.

45 Jain, Anil ed. Biometrics: personal identification in networked society. Boston: Kluwer Academic Publishers. Pág. 35. 1999.

Number en los Estados Unidos ha sido extendido a otros fines diferentes a los inicialmente autorizados ya que progresivamente se ha utilizado para aspectos relacionados con los impuestos, desempleo, beneficios pensionales, entre otros[46]. Woodward, por su parte, menciona un ejemplo de la historia de los Estados Unidos en donde información de un censo de población fue utilizada para fines no autorizados ni previstos inicialmente:

> "*En noviembre de 1941, casi dos semanas antes del ataque japonés en Pearl Harbor, el Presidente Franklin D. Roosevelt ordenó hacer un listado que incluyera los nombres y direcciones de todos los descendientes de japoneses nacidos y no nacidos en los Estados Unidos que estuvieran viviendo en dicho país. Para realizar dicho listado, se utilizó la información contenida en los censos de población de los años 30 y 40. En ese entonces, sin el uso de sistemas computarizados, se realizó dicho listado en una semana. En la primavera de 1942, el gobierno de los Estados Unidos obligó a todas las personas de descendencia japonesa, incluidos ciudadanos americanos, a dejar sus casas y ubicarse en unos ´relocations centres´ ubicados en la costa oeste de los Estados Unidos*"[47]

7- Desarrollos jurisprudenciales sobre el "habeas data" en Colombia

Pese a la consagración constitucional del habeas data y la libertad informática en la Constitución de 1991, Colombia no cuenta con una ley sobre la materia. Desde 1986 se ha presentado múltiples propuestas al Congreso sin que éstas se materialicen en ley estatutaria. En ausencia de legislación, la acción de tutela y el derecho de petición son las únicas herramientas con que cuentan los colombianos para exigir el respeto al habeas data y demás derechos conexos.

Con ocasión de casos reales que involucran el tratamiento de datos personales de muchos ciudadanos, la Corte Constitucional, a través de más de 110 sentencias, ha definido el alcance y características del habeas data así como las condiciones que deben rodear el tratamiento de los datos personales. La Corte ha incorporado en sus fallos los lineamientos contenidos en documentos internacionales emitidos por la ONU y la Unión Europea[48]. A continuación se hará una breve referencia a algunos principios constitucionales que deben observarse en el tratamiento de datos personales en general y para fines estadísticos en particular:

46 Davies, Simon. "*Touching big brother: how biometrics technology Hill fuse flesh and machines".* Artículo publicado en: Information Technology & People. Vol. 7. No. 4, 1994.

47 Woodward, John, "Biometric Scanning, Law & Policy: Identifying the concerns-drafting the biometric blueprint". University of Pittsburgh Law Review. Pág. 395. 1997.

48 Sobre este aspecto se sugiere consultar el siguiente texto del autor: Data protection: Panorama nacional e internacional. Capítulo de libro publicado en "Internet, Comercio Electrónico & Telecomunicaciones" (Legis, junio de 2002).

- ***Del deber constitucional de administrar correctamente y proteger los archivos o bases de datos que contengan información personal:*** Dado los riesgos que genera el tratamiento inadecuado de los datos personales, la Corte ha señalado como deber imperativo de los administradores de bancos de datos el administrar correctamente los sistemas de información, manuales o sistematizados, que contengan datos personales: *"En concepto de esta Corporación existe un deber constitucional de administrar correctamente y de proteger los archivos y bases de datos que contengan información personal o socialmente relevante"*[49]. Esta obligación constitucional debe ser observada, entre otros, por le DANE y quienes administren la información recolectada en los censos.
- ***Principio de utilidad:*** Este busca restringir la posibilidad de mantener información personal sin una función jurídicamente amparable. Por eso, según la Corte, "*el acopio, el procesamiento y la divulgación de los datos personales debe cumplir una función específica, que implica la satisfacción de un interés legítimo determinado por la importancia y utilidad de la información*". En virtud de lo anterior, señala la Corte, no es admisible "*el acopio, procesamiento y divulgación de datos personales que, al carecer de función, no obedezca a una utilidad clara o determinable o que no esté protegida por el ordenamiento jurídico*"[50]. En el caso de los censos, la utilidad de los mismos está señalada en la ley 79 de 1993[51] sobre la cual nos referiremos mas adelante.
- ***La persona como titular de sus datos personales:*** Desde la primera sentencia sobre el tema (T-414 del 16 de junio de 1992), la Corte Constitucional ha aclarado que la persona, y no el administrador del banco de datos, es el titular y propietario del dato personal. En dicha sentencia, la Corte precisó que frente al dato personal no puede aplicarse en todo su rigor el derecho clásico de la propiedad y que la sola búsqueda o hallazgo de un dato no significa que se ha producido simultáneamente su apropiación exclusiva y, por tanto, la exclusión de toda pretensión por parte del sujeto concernido en el dato. Esto significa que, entre otras, los datos personales contenidos en bases de datos o centrales de información no son bienes o activos del

49 Corte Constitucional, sentencia T-227 del 17 de marzo de 2003. M.P. Dr. Eduardo Montealegre Lynett

50 Cfr. Corte Constitucional, Sentencia C-185/03. En esta sentencia, la Corte, con ocasión de una demanda parcial de incostitucionalidad del artículo 54 del Decreto Ley 1250 de 1970, analizó si la norma demandada, al establecer la obligación de certificar las inscripciones canceladas que constituyen información considerada como negativa (principalmente la que revela la existencia de embargos) desconoce los principios de utilidad y de temporalidad de la información, propios del derecho al habeas data, o si, por el contrario, constituye un desarrollo constitucionalmente legítimo de los principios de publicidad de la función pública registral y de seguridad jurídica.

51 *"por la cual se regula la realización de los Censos de Población y Vivienda en todo el territorio nacional"*.

administrador del banco de datos. Por eso, salvo que la ley o el titular del dato lo autorice, el DANE no puede hacer lo que quiera con la información (venderla, cederla, entre otras). Adicionalmente, al ciudadano, como titular de sus datos personales, se le confieren derechos y privilegios para exigir ante los administradores de bancos de datos y los jueces el tratamiento leal, lícito y adecuado de su información.

- ***Autorización:*** Se ha establecido como principio fundamental del tratamiento de datos personales la obligación del administrador del banco de datos de obtener previamente la autorización del titular del mismo para que ellos sean incluidos en la base de datos. De lo contrario, esos datos se deben borrar inmediatamente.[52] En otras palabras, para considerarse lícita la recolección de datos personales, es necesario obtener la autorización de la persona. Reiteradamente la Corte ha ratificado no sólo que el consentimiento del titular de la información es esencial para salvaguardar los derechos del titular de la información sino que el receptor de la información (administrador del banco de datos) debe informar a la persona (titular del dato) cómo, ante quién, desde cuándo y por cuánto tiempo su autorización será utilizada[53]

  El principio de autorización no es absoluto. Existen casos en los que debido a las funciones legales que deben cumplir algunas entidades del Estado, no es necesaria la autorización del titular del mismo. Uno de ellos, es precisamente, el caso de los censos. El artículo 5 de la ley 79 de 1993 obliga a los ciudadanos a suministrar al DANE los datos solicitados en el desarrollo de Censos y Encuestas. El incumplimiento de este deber puede ser sancionado por el DANE con multas que oscilan entre uno (1) y cincuenta (50) salarios mínimos mensuales[54] .

- **Derecho de acceso:** Éste comprende las facultades que confiere el artículo 15 de la Constitución al habeas data: "*las personas tienen derecho no solamente a conocer y a rectificar, sino a actualizar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas o privadas. Lo primero implica la posibilidad que tiene el ciudadano de saber en forma inmediata y completa, cómo, por qué y dónde aparece cualquier dato relacionado con él; lo segundo significa que, si la información es errónea o inexacta, el individuo puede solicitar, con derecho a respuesta también inmediata, que la entidad responsable del sistema introduzca en él las pertinentes correcciones, aclaraciones o eliminaciones, a fin de preservar sus derechos fundamentales vulnerados; lo tercero implica que el dato debe reflejar la situación real de aquel*

52 Cfr. Corte Constitucional, Sentencia T-002/93

53 Cfr. Corte Constitucional, Sentencia T-592 del 17 de julio de 2003, C-993 de 2004 y T-526 de 2004

54 Cfr. Art. 6 de la ley 79 de 1993.

a quien aludé"[55]. Todo lo anterior significa que el DANE y cualquier entidad pública o privada debe permitir al ciudadano el conocimiento, la actualización y la rectificación de los datos personales recolectados con ocasión del cumplimiento de sus deberes.

- ***Exactitud y veracidad de la información:*** El artículo 20 de la Carta Política de 1991 consagra el derecho de informar y recibir información "veraz e imparcial". Estas condiciones de veracidad e imparcialidad también deben predicarse en el tratamiento de datos personales para fines censales o estadísticos. La información que se encuentre en un banco de datos debe ser permanentemente actualizada introduciendo en forma íntegra todas las actuaciones y situaciones relacionadas con los datos contenidos en los archivos.[56] La actualización y la rectificación de los datos contrarios a la verdad, son, en principio, obligaciones de quien maneja el banco de datos.[57] En cuanto al alcance de los términos "rectificar" y "actualizar", la Corte ha precisado que la expresión "rectificación" se refiere a la concordancia del dato con la realidad, mientras que el término "actualización" *"hace referencia a la vigencia del dato de tal manera que no se muestren situaciones carentes de actualidad"*[58].

- ***Relevancia y finalidad del dato.*** Para la Corte, todo dato se debe recolectar para una finalidad constitucionalmente legítima[59] *"definida de manera clara, suficiente y previa; de tal forma que queda prohibida la recopilación de datos sin la clara especificación acerca de la finalidad de los mismos así como el uso o divulgación de datos para una finalidad diferente a la inicialmente prevista"*[60]. La persona no sólo tiene derecho a autorizar la circulación de sus datos sino a limitar el uso de los mismos. Por lo tanto, la autorización debe ir acompañada de específicas y restrictivas finalidades dentro de las cuales la persona otorga su consentimiento. En otras palabras, los datos deben ser, de una parte, recogidos con fines determinados, explícitos y legítimos, y no deben ser

55 Cfr. Corte Constitucional, sentencias T-110/93; T-303/98 y T-321/00, entre otras. *En la sentencia T-309 de 1999 se agregó que "el derecho al habeas data, incluye la facultad de toda persona de solicitar y obtener, en un tiempo razonable, la corrección, complementación, inserción, limitación, actualización o cancelación de un dato que le concierne".*

56 Cfr. Las siguientes sentencias de la Corte Constitucional: T-615/95; T-176/95; T-443/94; T-094/95; T-094/95; SU-089/95; T-443/94; T-552/97; T-096ª/95; T-086/96; T-097/95; T-414/1992; T-008/93, T-022/93 y T-060/03

57 Cfr. Las siguientes sentencias de la Corte Constitucional: SU 082/95, SU-089/95 y T-310/03.

58 Cfr. Corte Constitucional, sentencias T-578/01 y t-268/02, entre otras.

59 Cfr. Corte Constitucional, Sentencia No. T-307/99

60 Cfr. Corte Constitucional, Sentencia No. T-729/02. En la sentencia C-993 de 2004 la Corte precisó el alcance del principio de la finalidad del dato.

tratados posteriormente de manera incompatible con dichos fines[61] y, de otra parte, adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben[62].

Según la Corte, el principio de relevancia supone: *"(i.) que sólo puede requerirse y revelarse la información que esté relacionada con las funciones legalmente atribuidas a la entidad que la solicita (..)y, (ii.) debe existir un vínculo directo entre los datos requeridos y la cuestión materia de análisis que justifica su recopilación"*[63]. Así, las entidades y recolectores de datos personales como el DANE deben justificar la pertinencia de tales datos, de manera tal que se demuestre la relación directa entre lo que se solicita y la finalidad del censo.

El principio de la finalidad, por su parte, según el fallo citado, exige que la información requerida y revelada sea *"(i.) estrictamente necesaria para cumplir los fines (...), y (ii.) sólo sea utilizada para los fines autorizados por la ley (...)"*[64]. En materia de censos, el artículo 5 de la ley 79 de 1993 incorpora este principio al ordenar al DANE no utilizar la información que recolecta para fines diferentes a los estadísticos: "*Los datos suministrados al Departamento Administrativo Nacional de Estadística DANE, en el desarrollo de los censos y encuestas, no podrán darse a conocer al público ni a las entidades u organismos oficiales, ni a las autoridades públicas, sino únicamente en resúmenes numéricos, que no hagan posible deducir de ellos información alguna de carácter individual que pudiera utilizarse para fines comerciales, de tributación fiscal, de investigación judicial o cualquier otro diferente del propiamente estadístico*".

- ***No discriminación y datos sensibles:*** La Corte ha manifestado que "*no puede recolectarse información sobre datos "sensibles" como, por ejemplo, la orientación sexual de las personas, su filiación política o su credo religioso, cuando ello, directa o*

61 La Legislación colombiana ha introducido y exigido el respeto del principio de finalidad del dato, tal y como se desprende del artículo 5 de la Ley 79 de 1993 que prohíbe al Departamento Administrativo Nacional de Estadística (DANE) suministrar los datos que obtiene en los censos para que sean utilizados para fines comerciales, tributación fiscal, de investigación judicial o cualquier otro diferente del propiamente estadístico.

62 En este sentido, la Corte ha precisado que la "información solicitada por el banco de datos, debe ser la estrictamente necesaria y útil, para alcanzar la finalidad constitucional perseguida. Por ello, los datos sólo pueden permanecer consignados en el archivo mientras se alcanzan los objetivos perseguidos. Una vez esto ocurra, deben desaparecer" (Cfr. Corte Constitucional, sentencia T-307/99, entre otras)

63 En sentencia T-440 del 29 de Mayo de 2003, la Corte Constitucional hizo alusión al principio de relevancia. En esa sentencia, la Corte entró a resolver el siguiente problema jurídico: ¿Se configura una vía de hecho cuando, durante el trámite procesal de una acción de grupo dirigida contra una entidad bancaria y encaminada a obtener la indemnización colectiva de los daños y perjuicios causados por cobros efectuados a sus usuarios, el juez decreta algunas pruebas que implican la revelación de datos confiados por estos últimos al banco?

64 En este sentido también se ha pronunciado la Corte en las sentencias T-307/99 y C-993/04

indirectamente, pueda conducir a una política de discriminación o marginación"[65]. Esta regla no es absoluta. El tratamiento de este tipo de datos se puede realizar bajo determinadas y excepcionales condiciones. Usualmente, es obligatorio garantizar un cuidado extremadamente especial en el almacenamiento y circulación de esta información. Su tratamiento únicamente puede realizarse por entidades autorizadas por la ley y para los fines indicados en la misma. En principio, no es clara la conexidad entre la recolección de información sensible y los fines del censo. En todo caso, si se piensa requerir al ciudadano este tipo de información, se deben adoptar medidas estrictas de seguridad y control con miras a evitar el uso impropio de dicha de información.

- ***De la responsabilidad del administrador del banco de datos:*** Los administradores de bancos de datos o centrales de información como el DANE están sometidos a una responsabilidad social que implica que la información que difundan sea veraz e imparcial y no atente contra los derechos fundamentales de los ciudadanos[66]. Mediante sentencia T- 729 de 2002, la Corte Constitucional señaló, de manera general, que "*la función de administrar una base de datos debe fundamentarse en los principios de libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad*"[67].

8 - El tratamiento de datos personales para fines estadísticos y en el sector público en general

Mediante decreto 1820 del 6 de agosto de 1990 se creó el Sistema Estadístico Nacional (SEN), con miras a que el Estado cuente con información estadística confiable y oportuna que sea útil en el proceso de planeación y toma de decisiones. El SEN es un organismo adscrito al DANE, el cual está conformado por las entidades productoras y por los principales usuarios de la información estadística. Su principal función consiste en coordinar en forma general la actividad estadística que adelanten las diferentes entidades del sector público y velar por la integración entre los productores y los usuarios de la información estadística.

65 Cfr. Corte Constitucional , Sentencia No. T-307/99

66 Cfr. Las siguientes sentencias de la Corte Constitucional : T-512/92 ; T-603/92; T- 609/92; T-048/93; T-050/93; T- 080/93 ; T-332/93; T-369/93; ST-479/93; C-488/93; ST-259/94; SU-056/95; ST-074/95; T-206/95; ST-602/95 y T-472/96

67 En este mismo sentido ver la sentencia T-310/03, en la que la Corte, entre otras, analiza la incidencia de los principios que orientan la administración de datos personales en el caso específico del registro de las órdenes de captura y su cancelación. Así mismo, en sentencia T-018 de 2005 la Corte recalcó que los errores operativos de un banco no los debe asumir el ciudadano.

A través del SEN se busca maximizar la información que reposan en banco de datos administrados por entidades gubernamentales con miras a superar vacíos de información y eliminar duplicidad de esfuerzos y recursos. Dentro de la gama de información se encuentran los datos personales para los cuales el ordenamiento jurídico demanda un tratamiento adecuado y diferencial con miras a evitar la vulneración de los derechos fundamentales de los ciudadanos.

En las siguientes líneas se hará referencia a la regulación nacional e internacional en cuanto al tratamiento de datos personales en el sector público con particular énfasis al tema de la reserva legal del dato estadístico.

8.1 El derecho de acceso a información pública y la información reservada.

Según el artículo 74 de la Constitución colombiana, las personas tienen derecho a acceder a los documentos públicos, salvo en los casos que establezca la ley. El artículo 15 de la ley 57[68] de 1985 limita este derecho frente a los datos reservados conforme a la Constitución y a la Ley. Así las cosas, que sólo el legislador tiene la atribución de darle el carácter reservado[69] a cierta información y de establecer las correspondientes limitaciones para acceder a la misma.[70]

La ley 57 de 1985 regula, entre otros, lo atinente al acceso de los ciudadanos a los documentos que se encuentren en las entidades públicas. Particularmente, el artículo 12 dispone que "*Toda persona tiene derecho a consultar los documentos que reposen en las oficinas públicas y a que se le expida copia de los mismos, siempre que dichos documentos no*

68 "*Por la cual se ordena la publicidad de los actos y documentos oficiales*". Publicada en el Diario Oficial No. 37056 del 12 de julio de 1985

69 Algunos ejemplos de información reservada en la legislación colombiana son: Las deliberaciones del Consejo Nacional de Seguridad (Ley 52 del 28 de diciembre de 1990, art. 22); Los archivos de las personas acogidas al programa de protección de testigos, víctimas e intervinientes en el proceso penal (Decreto 1843 del 13 de noviembre de 1992, art. 5); La información tributaria respecto de las bases gravables y la determinación privada de los impuestos que figuren en las declaraciones tributarias (Estatuto Tributario, art. 583); Las actas y temas tratados en el Consejo Nacional de Estupefacientes (Ley 30 del 31 de enero de 1986, art. 94); Los libros y papeles del comerciante (Código de Comercio, arts. 61-62); La historia clínica (Ley 23 de 1981, art. 34); Los datos suministrados al Departamento Administrativo Nacional de Estadística DANE, en desarrollo de los censos y encuestas (Ley 79 del 20 de octubre de 1993, art. 5) y el art. 75 del decreto 1633 de 1960 (Norma vigente a juicio del Consejo de Estado en concepto de la Sala de Consulta y Servicio Civil –Rad. 1209 del 27-IX-99.)

70 Cfr. CONSEJO DE ESTADO, Sala de lo Contencioso Administrativo, Sección Primera. Exp. 4155, 4379, 4150 y 4175. Sentencia del 29 de enero de 1998. C.P. Dr. Ernesto Rafael Ariza Muñoz.

tengan carácter reservado conforme a la Constitución o la ley, o no hagan relación a la defensa o seguridad nacional"[71]. *(Subrayo*).

Sobre los límites al derecho de acceso a documentos públicos la Corte Constitucional ha puesto de presente que "*(...) el derecho de acceso tiene, como todo derecho, algunos límites (...). En consecuencia, los funcionarios están autorizados para no permitir el acceso a aquellos documentos cuya consulta o comunicación pueda atentar contra secretos protegidos por ley, tales como los concernientes a la defensa y seguridad nacionales, a investigaciones relacionadas con infracciones de carácter penal, fiscal, aduanero o cambiario así como a los secretos comerciales e industriales. Por razones obvias, el acceso no es tampoco permitido cuando el contenido de los documentos vulnere el derecho a la intimidad consagrado en el artículo 15 de la Carta vigente, algunas de cuyas implicaciones ha tenido a bien señalar ya esta Corte, específicamente en cuanto concierne al hábeas data. Por todo lo anterior, el ejercicio del derecho al acceso a documentos públicos debe, pues, ceñirse a los postulados de la Constitución y la ley tal como lo dispone expresamente el artículo 74. Vale decir: sólo la Carta Fundamental y la ley pueden establecer límites al ejercicio de este derecho que, por supuesto, incluye la consulta de los documentos in situ y no sólo, como pudiera pensarse, la solicitud de copias de los mismos.*"[72] (Subrayo)

Es importante anotar que de conformidad con el artículo 20 de la ley 57 de 1985 el "*carácter reservado de un documento no será oponible a las autoridades que lo soliciten para el debido ejercicio de sus funciones*", correspondiendo a la autoridad que requiera dicha información la obligación de "*asegurar la reserva de los documentos que lleguen a conocer*" en desarrollo de lo prescrito en el artículo aludido. A título ilustrativo, la Corte ha señalado que en aplicación de dicha norma "*en el curso de un proceso penal o disciplinario la autoridad competente levanta el velo de la reserva y accede a la información secreta para los propósitos de la investigación*"[73]: ¿Significa lo anterior que la información de los censos podrá ser circulada a otras entidades públicas?

61 La reserva legal sobre cualquier documento cesa a los treinta (30) años de su expedición. Posteriormente dicho documento adquiere carácter histórico de manera que podrá ser consultado por cualquier ciudadano y la autoridad que esté en su posesión adquiere la obligación de expedir a quien lo demande copias o fotocopias de mismo (Art. 13 de la ley 57 de 1985)

72 Cfr. Corte Constitucional, Sentencia T-473 de 1992. M.P. Ciro Angarita Barón.

73 Cfr. Corte Constitucional. Sentencia C-872 del 30 de septiembre de 2003. M.P.: Dra. Clara Inés Vargas Hernández. En esta sentencia, la Corte analizó la constitucionalidad del decreto 1799 del 14 de septiembre de 2000 "Por el cual se dictan las normas sobre evaluación y clasificación para el personal de Oficiales y Suboficiales de las Fuerzas Militares y se establecen otras disposiciones»:

«*Artículo 27. Carácter: Son documentos elaborados por las autoridades evaluadoras y revisoras en los que se consignan informaciones y juicios de valor acerca de las condiciones personales y profesionales de los oficiales y suboficiales regidos por este decreto. Los documentos de evaluación tienen carácter de reservado salvo para las partes que intervienen en el proceso.*

Artículo 42. Reserva. Las sesiones decisorias de la junta calificadora y las decisiones tomadas tienen carácter reservado, así como los documentos en que ellas consten.»

La existencia de información que no debe ser conocida por el público (reservada) es una constante en todos los sistemas de gobierno. Quien posea este tipo de información tiene la obligación de abstenerse de no publicar, comunicar ni dejar consultar la misma a terceros o personas no autorizadas. Igualmente, debe adoptar medidas administrativas, técnicas y organizacionales tendientes a impedir el acceso no autorizado por la ley o la divulgación o utilización ilegal de dicha información. El incumplimiento de los deberes que impone el tratamiento de información sujeta a reserva es sancionado penal[74] y disciplinariamente[75] por la legislación colombiana.

Por regla general, sólo puede acceder a la información reservada los funcionarios autorizados para el efecto que pertenezcan a la entidad que posea la información y el titular de la información en ejercicio del derecho fundamental del habeas data. Igualmente, pueden tener acceso funcionarios de otras entidades en cumplimiento de expresos mandatos legales y para fines específicos. Así por ejemplo, para el cabal cumplimiento de su finalidad y funciones el DAS tiene "*acceso a todos los documentos y bases de datos de la administración pública, cualquiera que sea el orden al que pertenezca, relativas a hechos, circunstancias, actuaciones, personas y organizaciones que puedan menoscabar la seguridad nacional*"[76] . (Subrayo). Esta norma diluye los efectos de la reserva estadística de los datos del censo de manera que el DAS podría acceder a la misma. En consecuencia, el secreto sobre la información censal no es absoluto.

En todo caso, es preciso determinar si existe una norma particular que regule el tratamiento de determinada información catalogada como reservada para poder precisar el alcance concreto que tiene la misma así como el uso que se le puede dar y las personas que pueden conocerla.

8.2 Panorama nacional de la reserva estadística.

El artículo 5 de la Ley 79 de 1993 precisa que: "*Los datos suministrados al Departamento Administrativo Nacional de Estadística DANE, en el desarrollo de los censos y encuestas, no podrán darse a conocer al público ni a las entidades u organismos oficiales, ni a las*

74 El Código Penal colombiano (ley 599 de 2000) consagra los siguientes delitos: (i) *Divulgación y empleo de documentos reservados (art. 194); (ii) Revelación de secreto (Art. 418); (iii) Utilización de asunto sometido a secreto o reserva (Art. 419); (iv) Utilización indebida de información oficial privilegiada.* (art. 420); (v) *Utilización indebida de información obtenida en el ejercicio de función pública.*(art. 431)

75 Cfr. Ley 734 de 2000 arts. 23, 34, 35. Los funcionarios públicos están obligados a (i) utilizar la *información reservada a que tengan acceso por razón de su función, en forma exclusiva para los fines a que están afectos, y (ii) custodiar y cuidar la 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" (Destaco)*

76 Art. 39 del decreto 218 de 2000

autoridades públicas, sino únicamente en resúmenes numéricos, que no hagan posible deducir de ellos información alguna de carácter individual que pudiera utilizarse para fines comerciales, de tributación fiscal, de investigación judicial o cualquier otro diferente del propiamente estadístico" (Subrayo)

Esta disposición de carácter especial y excepcional deja claro que la información que el DANE recopile debe suministrarse de manera impersonal con miras a que no se identifique a la persona a la cual corresponden los datos y no se utilice la información para fines distintos de los estadísticos. Esto, como se anotó, no es absoluto frente a investigaciones que adelante el DAS.

La Sala de Consulta y Servicio Civil del Consejo de Estado se pronunció sobre el alcance de la reserva legal estadística[77] en los siguientes términos: (i) De la información obligatoria recogida en censos y encuestas debe distinguirse aquella que se remite directa e indirectamente al ámbito privado de la persona, cuyos datos individuales "*en ningún caso podrán darse a conocer por prohibición expresa del legislador*". La información que no es de carácter individual puede suministrarse desagregadamente (datos globales) *"sin que en ningún caso se ponga siquiera en peligro el derecho a la intimidad"* permitiendo traslucir o revelar información individual; (ii) El solo hecho de emplear encuestas para recolectar información no le imprime automáticamente el carácter de reservado a la información. El dato individual sujeto a reserva "*es aquel que deber ser suministrado obligatoriamente, pertenece a la esfera privada de la unidad estadística (persona natural o jurídica) y por tanto su conocimiento puede perjudicarla en cualquier forma, razón por la cual únicamente autoriza su inclusión en resúmenes numéricos*"; (iii) *"La reserva estadística impide el conocimiento de los datos mencionados no sólo al público en general sino a las entidades u organismos oficiales y a las autoridades públicas"*. y (iv) El dato estadístico individual únicamente puede ser utilizado para fines "estrictamente estadísticos". Estos dos últimos desarrollos guardan relación con el principio de finalidad del dato y el fenómeno de funtion creep vistos anteriormente.

8.3 La reserva estadística en el derecho comparado

Con miras a contar con un marco de referencia sobre los desarrollos de la función y la reserva estadística en el derecho comparado, a continuación se presenta un resumen de las principales conclusiones sobre los aspectos que rodean este

77 Consejo de Estado. Sala de Consulta y Servicio Civil. Ref. radicación No. 1209 (DANE. Alcance de la reserva estadística). Consejero Ponente. Dr. Flavio Augusto Rodríguez Arce. Bogotá, 27 de septiembre de 1999.

tema en los Estados Unidos, la Unión Europea en general y algunos países en particular (España, Inglaterra y Francia), Canadá y Argentina[78].

❑ Las experiencias internacionales en materia de regulación estadística muestran que el tratamiento de datos personales, el derecho a la información, el derecho a la intimidad son temas estrechamente ligados a la función estadística.

❑ Por regla general, el tema de los censos y estadísticas no es tratado en las Constituciones de los países analizados[79]. La mayoría de ellos poseen normas específicas que se refieren a los censos y estadísticas[80] a cargo de las entidades públicas. Estas disposiciones se deben integrar con otras de carácter general sobre la protección de datos personales o del derecho a la intimidad. En otros casos, las normas sobre el tratamiento de datos en general traen una referencia particular al uso de datos para fines de encuestas y estadísticas.

❑ La mayoría de los países analizados cuentan con un sistema centralizado[81] de los censos y estadísticas en el que una entidad estatal especializada se encarga del tema[82]. En otros, el sistema gubernamental opera descentralizadamente[83].

78 Un estudio detallado sobre la regulación del tema en cada uno de los países consultados puede consultarse en el siguiente texto del autor: Fundamentos jurídicos del sistema nacional de información respecto del tratamiento de datos personales en el sector público en general y para fines estadísticos en particular. Bogotá, enero de 2004

79Sólo las constituciones de los Estados Unidos y España hacen referencia al tema.

80 España, Inglaterra, Francia, Canadá y Argentina.

81 Incluso existen sistemas centralizados que coordina la actividad estadística entre países. En la Unión Europea, por ejemplo, LA EUROSTAT (Oficina Estadística de las Comunidades Europeas) es la autoridad comunitaria encargada de garantizar el suministro de estadísticas para los objetivos políticos comunitarios. Su tarea principal consiste en la recopilación y la difusión de una información pertinente, en tiempo útil, sobre una amplia gama de temas sociales, económicos y medioambientales para apoyar las políticas actuales y futuras de la Unión Europea (UE). En el cumplimiento de su misión, Eurostat debe respetar los principios de imparcialidad, fiabilidad, pertinencia, relación coste/eficacia, secreto estadístico y transparencia

82 España, Inglaterra, Canadá, Argentina

83 En los Estados Unidos, por ejemplo, almenos nueve departamentos de agencias federales tienen oficinas especializadas que se encargan de la función de recolección, tratamiento y publicación de información estadística respecto de determinados temas: El Departamento de Agricultura (National Agricultural Statistics Service and Economics Research); el Departamento de Comercio (Bureau of Economic Analysis and Bureau of the Census); el Departamento de Educación (National Center for Education Statistics); el Departamento de Energía (Energy Information Administration); el Departamento de Salud (National Center for Healt Statistics); el Departamento de Justicia (Bureau of Justice Statistics); el Departamento del Trabajo (Bureau of Labor Statistics); el Departamento de Transporte (Bureau of Transportation Statistics) y el Departamento del Tesoro (Statistics of Income División of the Internal Revenue Service). Estas agencias operan de conformidad con sus estatutos, los cuales las autorizan para colectar, procesar y publicar información estadística.

❑ En cuanto al acceso a la información que reposa en entidades públicas, las normas de los países prevén como regla general el libre acceso y publicación de la misma salvo casos en que exista una excepción o limitación legal. La información recolectada para fines estadísticos se cataloga como reservada o confidencial[84] y por ende no es de libre acceso a terceros. Adicionalmente, también se consagran disposiciones tendientes a que las entidades gubernamentales no permitan el acceso y publicación de información que pueda afectar el derecho a la privacidad de las personas (por ejemplo los archivos médicos). Finalmente, existen normas que prohíben la difusión de información de cualquier persona cuya revelación puede razonablemente poner en peligro su vida o su seguridad física.

❑ Los siguientes son algunos de los principios comunes que irrigan el tratamiento de datos personales para fines estadísticos en los países estudiados: (i) la información recolectada no puede ser utilizada, parcial o totalmente, para propósitos diferentes del estadísticos ni para tomar alguna decisión respecto del encuestado; (ii) El encuestado tiene derecho a obtener acceso a la información que repose sobre él y a conocer la protección legal que se da a su información así como los usos que tendrá la misma; (ii) La entidades estatales sólo pueden recolectar la información estrictamente necesaria para alcanzar los objetivos del censo o encuesta[85].

❑ En términos generales, las legislaciones hacen referencia al alcance del "secreto estadístico" que pretende la no divulgación o acceso a los datos personales recogidos para fines estadísticos. Salvo algunas excepciones, el secreto estadístico también aplica frente a otras entidades públicas.

❑ Por considerarse reservados o confidenciales los datos personales para fines estadísticos, las regulaciones consagran obligaciones específicas en cabeza de los funcionarios públicos o de las entidades públicas que tratan dichos datos con miras a: (1) No usar la información recolectada para fines diferentes al estadístico; (2) No realizar ninguna publicación de la información de manera que de la misma, directa o indirectamente, se pueda identificar la persona que proporcionó la infor-

84 En los Estados Unidos, por ejemplo, la "*Confidential Information Protection and Statistical Act*" de 2002 señala que cuando las personas entregan su información bajo reserva de confidencialidad para fines estadísticos ello significa que la información se debe tratar como confidencial y no se puede usar para iniciar acciones legales o administrativas contra el titular de la información. El debilitamiento de la aplicación del principio de protección de información proporcionada bajo promesa de confidencialidad (*Pledge of confidentiality*) por parte de la entidad gubernamental puede producir efectos adversos respecto de la exactitud e integridad de los análisis estadísticos. Por eso, señala la norma, el respeto de dicho principio es esencial para garantizar y estimular la cooperación de las personas en los programas estadísticos.

85 Estos están contenidos en las legislaciones de Estados Unidos, la Unión Europea, España, Inglaterra,

mación para fines estadísticos, y (3) No permitir que terceros examinen los reportes individuales de los censos o encuestas[86].

❑ La legislación también apunta a crear una cultura de protección de los datos estadísticos entre los funcionarios encargados del tratamiento de los mismos. Así por ejemplo, se busca lo siguiente: a) Enfatizar en los funcionarios la importancia de proteger la confidencialidad de la información; b) Capacitar a los funcionarios respecto del alcance de su obligación legal de proteger la confidencialidad de la información que permita revelar la identidad de los encuestados y en cuanto a los procedimientos establecidos para cumplir dicho cometido; c) Implementar medidas físicas y tecnológicas para garantizar la confidencialidad de la información; d) Capacitar los funcionarios para que cumplan estrictamente los protocolos o condiciones bajo los cuales se puede compartir información confidencial para determinados fines autorizados por la ley, adoptando medidas que obliguen al destinatario de la información mantener la confidencialidad de la misma y utilizarla únicamente para fines estadísticos.

❑ En algunos casos, las copias de los censos o encuestas son "inmunes" de procesos legales y no podrán, salvo autorización del titular de la información, ser utilizadas como prueba o utilizada para ningún propósito respecto de algún proceso, acción, demanda u otro procedimiento administrativo o judicial.

❑ De las normas revisadas se deriva una tendencia a fortalecer la confianza y cooperación de las personas mediante el respecto de la privacidad y el mantenimiento de la confidencialidad de la información recolectada en las encuestas.

❑ Existen disposiciones tendientes a diluir la reserva o confidencialidad de la información estadística en casos excepcionales como la investigación de delitos[87]. El receptor de dicha información está obligado a mantener la reserva o confidencialidad de la misma.

❑ Algunos países cuentan con normas especiales tendientes a que el administrador de los datos implemente sistemas de seguridad para evitar el acceso, uso, manipulación, etc de la información[88].

86 Cfr. Por ejemplo, la "Confidential Information Protection and Statistical Act" de los Estados Unidos

87 La USA Patriot Act de 2001, por ejemplo, permite al Fiscal General, a petición de un Juez, ordenar al Secretario del Departamento de Educación que la National Center for Education Statistics (NCES) le suministre información confidencial sobre los estudiantes para fines de investigación del delito de terrorismo. Esta información debe ser tratada por el Fiscal General como confidencial.

88 La *Federal Information Security Management Act* de 2002 de los Estados Unidos, por ejemplo, propende por la adopción de sistemas de seguridad a fin de, entre otras, proteger la información y los sistemas de información de accesos, usos, divulgación, modificaciones o destrucciones no autorizadas con miras a garantizar la integridad, confidencialidad y disponibilidad de la información. La preservación de la confidencialidad de la información se traduce en crear sistemas de restricción de acceso y divulgación de información para proteger la privacidad.

9- Conclusiones

Las bases de datos son el eje del funcionamiento de un Estado moderno y del denominado "e-government". Un sistema de información confiable y completo en cabeza de la administración pública apoyaría procesos públicos eficientes basados en las tecnologías de información. El tratamiento de datos personales para el cumplimiento de los cometidos constitucionales en general, y para fines estadísticos en particular, es un tema estrechamente ligado al habeas data y al data protection porque en la realización de los mismos el administrador de la información personal debe adoptar medidas con miras a no conculcar algunos derechos fundamentales de las personas.

La historia mundial ha constatado los efectos nefastos que puede generar el uso indebido de los datos personales y las tecnologías para su tratamiento. Las dolorosas lecciones aprendidas de lo sucedido en la II Guerra Mundial con la tecnología IBM y de la orden del Presidente Roosevelt en 1941 respecto de los censos de población son realidades que no debemos olvidar. Ellas nos permiten afirmar que cualquier esfuerzo para lograr un tratamiento adecuado de datos personales es binvenido pero insuficiente frente a los insospechados propósitos de algunos administradores de información personal y el sigilo o secreto que rodea la recolección y circulación de datos personales

El administrar correctamente y proteger los archivos y bases de datos que contengan información personal o socialmente relevante es un deber constitucional que implica obligaciones. En desarrollo de lo anterior, organismos internacionales como la ONU, la OECD y el Parlamento Europeo, entre otros, al igual que la Corte Constitucional colombiana han expedido o desarrollado una serie de principios y reglamentaciones relacionadas con el tratamiento de datos personales a través de bases de datos públicas o privadas.

Regulaciones internacionales en materia estadística muestran que el tratamiento de datos personales, el derecho a la información y el derecho a la intimidad son temas fundamentales que están estrechamente ligados a la función estadística. Adicionalmente, es una constante que datos personales obtenidos para fines estadísticos no deben utilizarse para propósitos diferentes, a menos que una ley o el titular lo autorice.

El tratamiento de datos personales genera riesgos en cabeza del titular de la información personal. Para alcanzar un tratamiento adecuado de los datos personales de los ciudadanos no es suficiente fijar políticas e implementarlas a través de normas o directivas. Se debe ir más allá. Es necesario capacitar a los funcionarios públicos con miras a crear una cultura organizacional que propenda por un comportamiento ético y legal en el cumplimiento de las funciones que involucren el uso de datos

personales. Si el funcionario no entiende el problema o los riesgos que puede llegar a causar por su indebida gestión muy difícilmente se comprometerá con esta cultura y el ciudadano será, en últimas, el afectado. Por eso, al igual que sucede en otros países en Colombia se debería enfocar esfuerzos a: (i) Capacitar a los funcionarios respecto del alcance de su obligación legal de proteger la información confidencial y de la importancia de proteger este tipo de protección; (ii) Recalcar en los funcionarios que la eventual vulneración de los derechos fundamentales de los ciudadanos puede ser ocasionada por sus actuaciones ilegales o no éticas en el tratamiento de los datos personales que accedan, conozcan o manipulen con ocasión del cumplimiento de sus funciones; (iii) Enfatizar en los funcionarios que es imprescindible que respeten las normas y principios que rigen el tratamiento de datos personales; (iv) Preparar los funcionarios para que cumplan estrictamente los protocolos o condiciones bajo los cuales se puede compartir información confidencial para determinados fines autorizados por la ley, adoptando medidas que obliguen al destinatario de la información mantener la confidencialidad de la misma y a utilizarla únicamente para fines estadísticos; (v) Dejar claro que, en todo caso, el uso indebido de información personal catalogada como confidencial es una conducta muy grave que acarrea sanciones disciplinarias y penales.

Catalogar como reservada determinada información personal es una garantía del ciudadano que blinda dichos datos personales de accesos no autorizados y limita los usos de los mismos. Por eso, normas nacionales e internacionales se enfocan a que, salvo autorización de la persona, la información suministrada para fines estadísticos: a) Se utilice para dicha finalidad y no para otros propósitos; b) No se divulgue de forma tal que permita identificar la persona que suministró la información.

El deber de reserva estadística o el denominado secreto estadístico guarda directa relación con el tratamiento de datos personales, particularmente en lo que respecta a la circulación del dato y al principio de finalidad. El principio de finalidad significa que el uso de los datos debe estar limitado a los fines para los cuales fueron recolectados, o a otros que fuesen consentidos o autorizados legalmente. Adicionalmente, los datos personales recolectados deben ser pertinentes respecto de la finalidad del tratamiento de la información personal. Dicho deber también obliga al administrador del dato a no dar a conocer o circular información personal amparada por la reserva o el secreto estadístico a terceros no autorizados por el titular del dato o por la ley.

Tratándose de información catalogada por la ley como reservada, no es procedente que quien la administra permita su consulta o entregue copias de la misma a personas no autorizadas. No obstante, excepcional y explícitamente existen algunas situaciones en las que se puede permitir el acceso a este tipo de

información: a) Cuando el peticionario es el titular del dato y en ejercicio del artículo 15 de la Constitución desea conocer, actualizar o rectificar su información personal; b) Cuando la ley lo autorice. En este último evento, corresponde al administrador de la información constatar el fundamento legal que lo obliga a suministrar o permitir acceder a esa información que reposa en sus archivos o bancos de datos manuales o sistematizados.

Dependencias internacionales que manejan información estadística consagran dentro de sus metas estratégicas el fortalecimiento de la confianza y cooperación de las personas mediante el respecto de la privacidad y el mantenimiento de la confidencialidad de la información que recolectan. Se considera que el no respetar la confidencialidad de la información que la persona entrega para fines estadísticos puede producir efectos adversos respecto de la calidad de la información o de la disposición de la persona para suministrar sus datos personales. Por eso, el respeto del deber de confidencialidad es una condición esencial para garantizar y estimular la cooperación de las personas en los programas estadísticos.

Es imprescindible adoptar y fortalecer medidas reglamentarias, administrativas, técnicas y organizacionales necesarias para la protección física e informática de los datos confidenciales con el propósito de mitigar cualquier riesgo de divulgación ilícita o la utilización para fines no estadísticos. En los eventos en que sea permitido el acceso a datos reservados o confidenciales también es importante adoptar medidas para impedir que con ello se menoscabe la protección física y lógica de los datos o se realice una divulgación o utilización ilegal para fines distintos de aquellos para los que se concedió el acceso. En todo caso, se recomienda que los datos consultados no contengan información que permita la identificación directa de los encuestados.

10 Bibliografía

¨ Cavoukian, Ann and Tapscott, Don. **Who knows: safeguarding your privacy in a networked world**. Random House of Canadá. Toronto, 1995.

¨ Dávara Rodríguez, Miguel Angel. **Derecho Informático**. Editorial Aranzadi, Pamplona. España. 1993

¨ Davies, Simon:

¨ **"Re-engineering the right to privacy: how has been transformed from a right to a commodity"**. Artículo publicado en: Agree and Rotenberg ed. Technology and privacy: The new landscape. Cambridge: MIT Press, 1997.

¨ **"*Touching big brother: how biometrics technology Hill fuse flesh and machines*"**. Artículo publicado en: **Information Technology & People**. Vol. 7. No. 4, 1994.

¨ Diffie, Whitfield. **The impact of a secret cryptographic standard on encryption, privacy, law enforcement and technology**. 1993

¨ Electronic Privacy Information Center (EPIC). Privacy & Human Rights: An internacional survey of privacy laws and developments. Washington, SC, USA. 2002 y 2003.

¨ Frosini, Vittorio. Informática y Derecho. Editorial Temis. Bogotá. 1988.

¨ Grupo Europeo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales. Primer **informe sobre la aplicación de la Directiva sobre Protección de Datos (95/45 CE)**. /*COM/2003/265: Mayo de 2003.

¨ Grupo Europeo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales. **Primer informe sobre la aplicación de la Directiva sobre Protección de Datos (95/45 CE)**. /*COM/2003/265: Mayo de 2003

¨ Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho de la Universidad de los Andes. **Internet, Comercio Electrónico & Telecomunicaciones**. Editorial Legis. Bogotá, junio de 2002.

¨ Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho de la Universidad de los Andes. **Derecho de Internet & Telecomunicaciones.** Editorial Legis. Bogotá, noviembre de 2003.

¨ Gutiérrez Gómez, María Clara. **Hacia el gobierno electrónico: elementos para el desarrollo de una política estatal**. Artículo publicado en el libro "Derecho de Internet & Telecomunicaciones" del "Grupos de Estudios en Internet, Comercio Electrónico y Telecomunicaciones (GECTI)" de la Facultad de Derecho de la Universidad de los Andes. Bogotá, Legis, noviembre de 2003.

¨ Isenberg. Doug. **The Giga Law: Guide to the Internet Law**. Random House Inc, edition. USA, 2002.

¨ Jackson, Davey & Sykes. **Legal problems of International Economic Relations**. Tercera edición. West Publishing Co. Pág. 991. Estados Unidos. 1995.

¨ Jain, Anil ed. **Biometrics: personal identification in networked society**. Boston: Kluwer Academic Publishers. Pág. 35. 1999.

¨ Jordan M. Blanke. **"Safe Harbor" and the European Union´s Directive on Data Protection**. Albany Law Journal of Science & Technology. 11 Alb. L.J. Sci. & Tech. 57. (69) 2000.

¨ Kayser, Pierre. **La protection du secret de la vie privee**. Económica. París, 1983.

¨ Madrid-Malo, Mario. **Derechos fundamentales**. Documento ESAP, Santafé de Bogotá,1991

¨ Millard, Christopher y Ford, Mark. **Data protection Laws of the world.** Sweet & Maxwell. Londres. 1999.

¨ Millard, Christopher. "*Data protection and the internet*". Artículo publicado en **Computer and Law**. Londres. Febrero-Marzo, 1999.

¨ Novoa Monreal, Eduardo. **Derecho a la vida privada y libertad de información: un conflicto de derechos.** Editorial Siglo XXI, Méjico, 1979.

¨ OECD (Organization for Economic Cooperation and Development). **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data** del 23 de septiembre de 1980.

¨ PRIVACY INTERNATIONAL. **Privacy and Human Rights 1999: An international survey of privacy laws and developments**. Londres y Washington. 1999.

¨ Pomed Sanchez, Luis Alberto. **El derecho de acceso de los ciudadanos a los archivos administrativos**. Madrid, 1989.

¨ Recasens Sincches, Luis. **Tratado general de filosofía del derecho**. Editorial Porrua, Méjico, 1970

¨ Remolina Angarita, Nelson:

¨ **Fundamentos jurídicos del sistema nacional de información respecto del tratamiento de datos personales en el sector público en general y para fines estadísticos en particular**. Bogotá, enero de 2004

¨ **Centrales de información, habeas data y protección de datos personales: Avances, retos y elementos para su regulación**. Capítulo de libro publicado en "Derecho de Internet & Telecomunicaciones" (Legis, noviembre de 2003).

¨ **Data protection: Panorama nacional e internacional.** Capítulo de libro publicado en "Internet, Comercio Electrónico & Telecomunicaciones" (Legis, junio de 2002).

¨ **La protección de datos personales en Colombia.** Artículo publicado en la Revista Tutela. Editorial Legis. Págs. 978-995. Tomo III, No. 28. Abril de 2002.

¨ **Biometrics and Human Rights**. LSE. Londres, 2000.

¨ **Avances tecnológicos de información y protección de datos personales.** Artículo publicado en la Revista Planeación & Desarrollo del Departamento Nacional de Planeación. Vol. 29. 1998.

¨ **El Habeas Data en Colombia**. Artículo publicado en la Revista de Derecho Privado No. 15 de la Facultad de Derecho de la Universidad de los Andes. Bogotá, 1994.

¨ Velásquez Bautista, Rafael. **Protección jurídica de datos personales automatizados**. Editorial Colex, Madrid, España. 1993.

¨ Tellez Valdez, Julio. **Derecho Informático**. Universidad Nacional Autónoma de México. Primera Edición. 1987.

¨ Universidad de los Andes. Anteproyecto de reglamentación de la reserva de los ciudadanos y la responsabilidad en el uso y almacenamiento de la información. Informe final. Bogotá. 1986.

¨ Wacks, Raymond:

¨ **Personal information: privacy and the law**. Oxford: Clarendon Press, 1989. **Law, Morality, and the private domain**. Hong Kong University Press, 2000.

¨ Woodward, John, "Biometric Scanning, Law & Policy: Identifying the concerns-drafting the biometric blueprint". University of Pittsburgh Law Review. 1997.

(In: http://www.pitt.edu/ ~ lawrev/59-1/woodward.htm)(as of 23/12/99)