El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica

Dr. Alfredo Chirino Sánchez
Director de la Escuela Judicial
Catedrático de Derecho Penal
Universidad de Costa Rica

Dr. Marvin Carvajal
Letrado de la Sala Constitucional
Profesor de la Universidad de Costa Rica

1. Introducción

El legislador ha emprendido, nuevamente, el tortuoso y difícil camino hacia la regulación del tratamiento de datos e informaciones personales, y lo hace cuando ya se empiezan a resquebrajar muchas de las instituciones tradicionales vinculadas al control institucional del procesamiento de datos. Tal parece como si la lucha de los costarricenses por alcanzar un estándar aceptable de tutela choca con los incesantes cambios que experimenta el mundo en lo tecnológico pero también en lo ideológico, y las condiciones están dispuestas para la desesperanza. Sin embargo, está claro que si no se inicia el camino hacia la tutela de los ciudadanos frente al tratamiento de sus datos personales, Costa Rica perderá una importante ventaja en el proceso de integración a un mundo cada vez más dependiente del conocimiento.

Después de los esfuerzos del ex diputado Dr. Constantino Urcuyo por impulsar una reforma a la Ley de la Jurisdicción Constitucional para incluir el recurso de habeas data como un instrumento formal de tutela de la persona frente al tratamiento de los datos personales, hoy plantea la diputada Margarita Penón una nueva iniciativa legislativa de gran interés para el país, donde se incluye una reflexión sobre los problemas del

moderno tratamiento de datos y las oportunidades que tiene el país para ofrecer un estándar de tutela acorde con las prescripciones internacionales.

Este nuevo Proyecto de Ley merece un estudio concienzudo que permita evaluar su capacidad de rendimiento frente a los retos que enfrenta el derecho de la protección de datos en el cambio de siglo.

Nos proponemos hacer un análisis pormenorizado del Proyecto, pero al mismo tiempo dar un vistazo a la situación internacional, con el fin de observar y aquilatar el alcance de las disposiciones incluidas en la versión preliminar de este proyecto.

La citación que se hará del articulado corresponde a la versión obtenida del Proyecto, correspondiente al mes de enero de 2003.

2. Los riesgos para los derechos fundamentales en la sociedad de la información

Panorama actual. Evolución tecnológica.
Los sujetos privados como manipuladores de datos personales.

El "valiente nuevo mundo" que se ha construido con las multicolores y extraordinarias herramientas de las tecnologías de la información y comunicación ha cambiado nuestra forma de entender la vida y nuestras relaciones. La intensidad del cambio puede sentirse en todas las actividades humanas, y es probable que las tendencias que hoy podemos estudiar terminen por profundizar las características de lo que se ha dado en llamar la "sociedad del conocimiento".

La aparente contradicción que nos ofrece la circunstancia actual se puede caracterizar en el presupuesto básico de la sociedad global que estamos viviendo, constituido por la relación directa existente entre el número de informaciones que circulan y el grado de democracia que es posible alcanzar. En efecto, una sociedad de conocimiento requiere que haya una circulación de informaciones y que dichas informaciones sean precisas,

adecuadas e idóneas para impulsar los procesos productivos y creativos de los países y de las personas. Al mismo tiempo tiene que tender a desarrollar las condiciones de autodeterminación de las personas, para que éstas puedan contribuir a mejorar todos los aspectos de la vida de convivencia, así como su propia vida. En un escenario como éste, resulta fundamental que el Estado de Derecho se transforme y se convierta en un facilitador de los procesos comunicativos e informativos, creando las condiciones para que los ciudadanos puedan informarse sobre todos los asuntos de su interés, proveyendo, al mismo tiempo, medios para que puedan darle valor agregado a las actividades en que participan. Ahí radica el enorme peligro. Tal apertura a la circulación de las informaciones enfrenta al individuo a numerosos riesgos de perder su intimidad y privacidad, a convertirse en un ciudadano de cristal, transparente al escrutinio y al control desenfrenados[1], ahora no sólo del Estado sino también de los particulares, hambrientos como aquél de informaciones sobre las personas para los más diversos fines sociales, muchos de ellos lícitos pero también para algunos no tan lícitos.

Es indudable que el ciudadano deja un rastro indeleble de su paso por todas y cada una de las actividades cotidianas, desde que tiene acceso a los cajeros automáticos, hasta cuando hace sus pagos por medio de tarjetas de crédito[2], desde que decide pedir un crédito o solicita un cambio de aceite para su vehículo hasta cuando plantea su gestión para obtener una pensión o accede a su página favorita en Internet. Casi no existe una posibilidad moderna de convertirse en un Robinson Crusoe y mantenerse alejado del peligro ser parte de un banco de datos. Por el solo hecho de ser ciudadano, y tener una

---

[1] Cfr. Krempl, Stefan, Grundpfeiler des Datenschutzes in der vernetzten Welt, en: http://www.heise.de/bin/tp/issue/

[2] Pagos que según información del periódico "Tiempos del Mundo", de los pasados días, van a ser delicadamente escrutados por un poderoso software en manos de la administración tributaria. Todos los movimientos financieros de una persona física o jurídica, al momento de hacer una transacción comercial, serán objeto de una revisión. Aquí se incluyen transacciones del ámbito privado como pago de alquileres, intereses y comisiones o servicios profesionales, los cuales quedarán al descubierto gracias a la trama de conexiones que puede establecer este software. Gracias a la declaración de impuestos, y a los datos y documentos ahí incluidos, podrá Tributación Directa no sólo comprobar la realidad de dichos pagos y erogaciones, sino también cruzar los datos y ver la realidad económica del contribuyente y probablemente de aquellos que tengan contacto comercial con él. Nadie duda de la importancia de mecanismos de este tipo para lograr una mejor recaudación, la cual, en efecto, ha sufrido notorias mejorías que la han llevado a alcanzar la suma de 1470 millones de colones, superando la meta prevista de 270 millones. Lo que sucede es que esta herramienta informática es demasiado poderosa como para restringirla únicamente a declaraciones "sospechosas". Es de esperar que probablemente se utilice para hacer investigaciones de rastros y para corroborar de manera aleatoria diferentes declaraciones, lo cual, gracias a la velocidad de procesamiento y a las capacidades de integración de datos, no tarden en dar con más de un contribuyente que tenga algo que explicar al fisco. Semanario "Tiempos del Mundo", Edición de Costa Rica, Semana del 16 al 22 de enero de 2003, Año 8, Nr. 3, p.2.

partida de nacimiento, ya nos podemos considerar incluidos en un ingente flujo de información, cuyas corrientes fluyen desde los bancos de datos de la administración a la de los particulares, y el proceso no parece tener límites.

Las autoridades utilizan también los mecanismos de las tecnologías de la información y la comunicación para vigilar y controlar a los ciudadanos, en una red que no diferencia entre personas respetuosas de la ley y aquellos sospechosos de cometer un delito[3]. En las redes de los sistemas de comparación de datos no existe forma de sostener un principio formal de inocencia y es probable, que en el transcurso de nuestra vida, a pesar de haber reconocido el valor de los dictados normativos, alguna vez hayamos formado parte de un elenco arbitrario, sutil y poderoso orquestado por un computador y su software de comparación de datos.

Los requisitos necesarios para construir una sociedad panóptica ya están presentes en nuestro mundo de la vida. Por doquier existen cámaras de video que graban nuestras actividades económicas, nuestros paseos por las góndolas del supermercado, por los parqueos de los centros comerciales o siquiera cuando nos interesamos por una prenda de vestir en numerosos comercios[4]. Hasta nuestro interés momentáneo en artículos anodinos como una específica marca de cereales o de galletas genera un interés comercial y de ahí su observación minuciosa por expertos de marketing. Ya se han desarrollado tecnologías que permiten, mediante minería de datos, recopilar también los comportamientos de las personas en el diario transitar por la "red de redes" Internet. Con los datos e informaciones obtenidas se pueden perfilar hábitos de consumo, intereses, actividades y pasatiempos y hasta actividades de investigación, los cuales pueden ser utilizados para los más diversos fines: desde el envío de correos con información de interés comercial, como para que las páginas de Internet "recuerden" nuestro paso e identidad y nos saluden efusivamente, invitándonos a otra partida emocionante de compras y diversión.

[3] Detallado sobre estos problemas cfr. Nogala, Detlef, Moderne Überwachungstechnologien. Zum Stand der Kunst, en: Bürgerrechte und Polizei/CILIP 60 (2/98).
[4] En este sentido, Weichert, Thilo, Gefangen im Netz der Datenbanken, en: http://www.humanistische-union.de/hu/10publikationenordner/grundrechte_report1997/06.htm

La red de redes no es nada más ni nada menos que la infraestructura sobre la que se está montando la nueva economía del conocimiento[5]. Las antiguas tradiciones jurídicas y la confianza, casi religiosa, en el funcionamiento de las normas, se revelan ante el nuevo panorama como naïve. Las reglas de la nueva cultura de la información deben construirse tomando en cuenta la dimensión e intensidad de los cambios que se están produciendo en todos los niveles de la vida de convivencia[6].

Culturalmente hemos asumido la percepción de que si no tenemos nada que ocultar, tampoco debemos preocuparnos porque otros sepan sobre nosotros, sobre nuestros gustos o apetencias. En general, consideramos que si entregamos datos a empresas financieras y bancarios, a servicios de pensiones, lo que estamos haciendo es contribuir al buen servicio que nos prestan, sin tomar en cuenta los riesgos que afrontamos ante tal liberalidad.

Los inmensos bancos de datos del Estado, pero también los construidos por los particulares, ofrecen un muestrario sorprendente de posibilidades de control, no sólo para desestimular a los que realizan actividades ilícitas, sino también para controlar a aquellos que eventualmente manifiesten algún interés sospechoso.

El gran reto de la nueva Era de la Información lo constituye, sin duda, como lo expone el Comisionado Federal para la Protección de datos de Alemania, Joachim Jacob[7], la interconexión que es posible alcanzar con la ayuda de la moderna tecnología, muy especialmente a nivel de los ciudadanos y sus hogares. Este reto obliga a repensar los medios utilizados hasta ahora para proteger la intimidad y la autodeterminación informativa de los ciudadanos. El desarrollo vertiginoso de la tecnología ha llevado a la moderna sociedad de la información a convertirse en una verdadera “aldea global”, la cual ha superado con creces la velocidad de adaptación que fue necesaria para alcanzar un uso global del teléfono o del fax. Hoy en día cada vez más personas hacen uso de la

[5] Cebrián, Juan Luis, La Red, Barcelona, Punto de Lectura, Santillana de Ediciones S.A., Tercera Edición, 2000, p. 19.
[6] Cebrián, La Red, p. 35
[7] Jacob, Joachim, Bundesbeauftragter für den Datenschutz, Dringender Handlungsbedarf für mehr Datenschutz auf dem nicht-öffentlichen Sektor, Pressemitteilung en: http://www.bfd.bund.de/aktuelles/pm19990504.html

Internet y la cantidad de información que circula en la Red se duplica cada cien días, según datos del Ministerio de Comercio de los Estados Unidos[8].

Aun cuando no puede confundirse Internet con las "autopistas de la información"[9], porque tal concepción dejaría por fuera otras formas de interconexión que se están produciendo en la actualidad, como ocurre en el mundo empresarial con las así denominadas "intranets", está claro que Internet tiene un rol muy claro en el proceso de dar forma a las nuevas relaciones informativas de los ciudadanos.

Junto al desarrollo de Internet debe indicarse que los servicios "multimedia", que integran texto, imágenes, video y sonido, también gozan de una excelente coyuntura, y han hecho posible, gracias a las generosas condiciones del ancho de banda disponible, que se ofrezcan servicios tales como "televideo", "telejuegos", "telecompras", "teleaprendizaje" y el "teletrabajo"[10].

Además de Internet y los servicios multimedia, cuentan también las famosas "tarjetas chip", las cuales han empezado a ser cotidianas en nuestra vida, dándonos acceso a cajeros automáticos, a llamadas telefónicas y recientemente al servicio de telefonía móvil GSM. Su función básica es ser almacenes de datos y en algunos casos, gracias al acondicionamiento de microprocesadores, pueden funcionar también como "tarjetas inteligentes".

En Costa Rica se ha anunciado recientemente[11] la introducción de una cédula de identidad "inteligente". La llamada "laser card" podrá contener una gran cantidad de información sobre el ciudadano y podrá ser utilizada como pasaporte, licencia para

---

[8] Junto a este crecimiento exponencial de los usos de Internet, debemos contar la creciente velocidad de procesamiento de los computadores y de los chips que les permiten las fantásticas prestaciones que hoy tienen. Los chips han visto incrementada su capacidad de procesamiento de una manera sorprendente, pasando de ejecutar 60.000 instrucciones por segundo a hacerlo en cientos de millones. En palabras de Nathan Myrvald, Vicepresidente para Tecnología de Microsoft, se trata de un panorama impresionante: Dentro de veinte años, un pc realizará en treinta segundos las tareas para las que hoy necesita doce meses. Dentro de cuante años, llevará a cabo en treinta segundos aquello para lo que hoy necesitaría un millón de años". Myrvald, Nathan, Intervención en el foro organizado por Variety y Time Warner, Nueva York, 1994, citado por Cebrián, La Red, p. 60.

[9] En este sentido Cebrián, La Red, p. 63.

[10] Kloepfer, Michael, Geben moderne Technologien und die europäische Integration Anlass, Notwendigkeit, und Grenzen des Schutzes personenbezogener Informationen neu zu bestimmen?, en: Revista Neue Juristische Wochenschrift, 1998, p. 21.

conducir, carné de oro y hasta para el carné de acceso a la seguridad social. Esto es, en términos generales, un medio para que la persona acceda a su integración con el grupo social, y para ser identificado en una serie de actividades altamente sensibles. Se estima que es posible que la tarjeta incluya la historia médica del ciudadano, incluyendo copias de los exámenes y pruebas a las que haya sido sometido[12].

La compañía interesada en el proyecto indica, con razón, que Costa Rica es un buen país para introducir esta tecnología, principalmente porque el número de cédula es el identificatorio más importante para los servicios que se prestan. En efecto, siendo que el número único de identificación de los ciudadanos en Costa Rica es el de la cédula de identidad, es muy fácil unir los sistemas para que todos puedan hacer uso del mismo documento para todos los servicios. Todo esto tiene el consecuente problema de control y abusos a los que ya se ha aludido en la primera parte de este estudio.

Otra información indica que pronto estarán disponibles en el mercado nacional "chips" que podrán ser implantados en el cuerpo de una persona, los cuales permitirán su ubicación en cualquier lugar, con la precisión del sistema de geoposicionamiento global (GPS). Este sistema, que se ha popularizado en otros países con los sistemas de navegación instalados en los vehículos, y que le permiten al chofer encontrar su camino aun en lugares que desconoce, ofrece ahora una poderosa arma en contra de los secuestros que se han popularizado en la región. Gracias a la cobertura satelital que ha hecho posible el servicio del GPS, ahora quienes temen ser objeto de un secuestro pueden confiar -en que con el "Verichip" que se les puede implantar en su cuerpo- podrán ser localizados en cualquier parte con una precisión extraordinaria[13].

---

[11] Ver nota en el periódico "La Nación", Lunes 27 de enero 2003, Sección Viva, ¿La cédula del 2010? en: http://www.nación.co.cr

[12] Según la publicación del Periódico "La Nación", esta tarjeta puede almacenar 4.1 megabytes de información, lo que representa unas 350 veces la capacidad de una tarjeta chip más modesta de 8n kilobytes, y más de 2500 veces la capacidad de un chip de un kilobyte. Los datos que ahí se escriban con la tecnología WORM (Write Once Read Many) nunca podrán ser borrados y siempre es posible agregar nuevos o actualizar los que hayan sido originalmente incorporados. Lo que permite presumir que los usos de esta tarjeta son altamente atractivos para todo tipo de empresas e instituciones, por ejemplo de seguros, bancarias y financieras, como también para el Estado y los órganos del control penal, solo para citar los ejemplos más sugerentes. Entre los países que ya la utilizan, destaca Estados Unidos, por ejemplo, quien de manera lógica la utiliza para emitir las así denominadas "green cards". Con idénticos objetivos quiere utilizarla también Canadá. Italia piensa darle uso como documento único de identificación.

[13] Ver nota en el periódico "La Nación, Domingo 2 de febrero de 2003, Revista Dominical, "Angel o espía", en: http://www.nacion.com/dominical/2003/febrero/02/home.html

Nadie duda de las enormes posibilidades que ofrece este instrumento para evitar secuestros o facilitar las pesquisas cuando un hecho de estos se comete, pero es el fin de la intimidad y la privacidad para las personas que portan este objeto, ya que no habrá lugar donde se puedan ocultar, o que lo hacen sin conocimiento de nadie, ya que los fieles satélites lo seguirán doquiera que vaya.

El chip también puede conservar información sobre la persona, incluso una imagen suya, así como detalles de su salud que podrían ser indispensables para un tratamiento médico, todo esto en su propio cuerpo y sin temor ya que el objeto es asumido por el cuerpo sin generar molestias. Pueden incluso imaginarse otros usos para el "Verichip" en el marco de medidas alternativas a la prisión, como en el caso de aquellos condenados a vivir en un determinado lugar o quedarse en su lugar de domicilio, gracias a este objeto podrían ser monitoriados en todo momento -y en el caso que infrinjan las medidas impuestas- puedan ser localizados por las autoridades. También, y en el mismo sentido, podría implantarse en aquellos sujetos condenados por un determinado delito, digamos sexual, y ser monitoriados en todo momento para evitar que cometan nuevos hechos o ser hallados en caso de sospecha de haber reincidido en su actividad criminal.

Lo dicho demuestra que los peligros que ya han sido reconocidos en otras latitudes ya están presentes en nuestro país, con el agravante de que aun no tenemos el desarrollo jurídico necesario para afrontarlos.

Estos servicios presentan a los ciudadanos diversos riesgos. Por ejemplo, en Internet la pregunta más importante es cómo pueden protegerse las informaciones y datos personales que circulan por ella de accesos ilícitos, de lectura no autorizada, de perfilado de usuarios y hasta de falsificaciones de los contenidos que los usuarios colocan en las páginas WEB. La transnacionalidad de la red, pero también su carácter arbitrario y desorganizado, hace que toda regulación jurídica enfrente serias dificultades, por lo que se ha optado por desarrollar una cultura de autoprotección para que los usuarios velen por sus derechos al hacer uso de todos los servicios que la World Wide Web le ofrece[14].

[14] Kloepfer, Technologien, p. 21.

Los servicios multimedia, por su parte, ofrecen diversos riesgos para los consumidores, siendo el primero, y quizá el más importante, el de la creación de perfiles de uso y consumo de los servicios por parte de las mismas compañías que ofrecen el acceso, así como la amplia posibilidad de enviar informaciones sensibles en fracciones de segundo. Los mecanismos ideales para enfrentar estos riegos van desde la actitud de los servicios de evitar usar muchos datos personales de los ciudadanos, así como establecer limitaciones para el almacenamiento de datos, además de reglas de anonimización y formas de pago que no permitan deducir la identidad de los usuarios a partir de patrones de pago o consumo.

Las tarjetas chip, igualmente, ofrecen la posibilidad de que sus propietarios dejen un rastro indeleble del uso que han hecho de ellas, y gracias a estos rastros es posible construir un perfil de la persona, de sus costumbres, así como del uso directo que hace de este instrumento. De la misma forma, el derecho de la protección de datos ha ido evolucionando para evitar que estas tarjetas chip sean utilizadas sin contemplar requerimientos mínimos tales como: restricciones de acceso para diferentes personas a nivel de software y hardware, así como creando, desde la programación de las tarjetas condiciones para que haya niveles de secreto de datos que fácilmente podrían afectar a los ciudadanos que las utilizan[15]. Entre estos niveles de secreto ha sido interesante la discusión propuesta en Alemania sobre el interés que podría tener, por ejemplo, un médico de urgencias de toda la información disponible en una tarjeta de salud sobre tratamientos recibidos por el paciente, historia de medicaciones específicas, datos sobre sus enfermedades venéreas para las cuales ha buscado ayuda, etc. Parece ser lógico que el médico de urgencias no debería tener acceso a todos esos datos, sino exclusivamente a aquellos que le permitan tomar decisiones inmediatas en relación con la situación de salud del paciente que ha sufrido un accidente.

Los desarrollos que se anuncian en el corto y mediano plazo permiten pensar en el así denominado “ubiquitous computing”, el cual podríamos traducir libremente como la “computación ubicua” que permite procesamiento de datos en todas partes. Es de cultura común el anuncio de aparatos domésticos que pueden acceder a Internet y ser

[15] Kloepfer, Technologien, p. 21.

controlados a través de ella. De hecho, la llamada "casa inteligente" está dispuesta para sustituir una serie de decisiones repetitivas de sus habitantes y tomar la delantera, por ejemplo, sobre cuáles bienes comprar y solicitarlos vía Internet al supermercado o controlar la temperatura interior del hogar o hasta poner la música que prefieren para calmar el estrés de un largo día de trabajo. Cada vez más, los instrumentos de nuestras vía cotidiana vienen dispuestos con suficiente poder informático para comunicarse entre sí, incluso sin cables y realmente no es posible determinar en todos los casos, qué tipo de datos podrían estarse transmitiendo unos y otros y quiénes podrían estar interesados en intervenir en tan conspicua comunicación[16].

3. Los retos del pasado en la regulación normativa y los problemas de hoy

La tarea legislativa que debe desplegarse para dar una efectiva protección al derecho a la autodeterminación informativa no sólo es compleja, sino también llena de dificultades por la amplitud y diversidad de los servicios de información que dependen hoy, en diversas formas y en diversa intensidad, de un procesamiento de datos personales.

Luego de la Sentencia sobre la Ley de Censos[17] del Tribunal Constitucional Federal Alemán, el antecedente más importante en dicho país sobre el desarrollo e importancia constitucional del derecho a la autodeterminación informativa, la doctrina no tardó en indicar que las áreas necesitadas de revisión y regulación abarcaban no sólo las tareas del Bundespost (Servicio de Correos Federal) sino también las relaciones jurídicas de información existentes en los Departamentos de Finanzas, las Autoridades encargadas de labores de Inteligencia y Seguridad (Sicherheitsbehörden), así como también los hospitales y centros de salud, solo para citar algunas áreas de urgente atención[18]. Solo en el tema de seguridad era necesario introducir normas específicas para regular el intercambio de información entre el Bundeskriminalamt (Policía Federal) y las

[16] Krempl, Grundpfeiler, p. 1
[17] Bundesverfassungsgericht (BVerfG): 1 BvR 209/83 ua, 15.12.1983 = BVerfGE 65, 1 ff.
[18] Con un detalle de la situación y necesidades de regulación en el ámbito federal como de los Länder alemanes en el año de 1989, siete años después de la sentencia del Tribunal Constitucional Alemán, y con la existencia de una Ley Federal de Protección de datos (Bundesdatenschutzgesetz), cfr. Simitis, Spiros, Konsequenzen des Volkszählungsurteils: Ende der Übergangsfrist, en: Revista Neue Juristische Wochenschrift (NJW), 1989, p. 21.

autoridades encargadas de fronteras (Grenzschutzbehörden), así como avanzar en un estándar legislativo que permitiera resolver arduos problemas con el tratamiento de la información realizado en el ámbito del proceso penal[19]. No sólo el problema del tratamiento de datos sin la autorización del afectado, así como la generosa práctica administrativa de compartir datos o de generar bancos de datos con todas las informaciones imaginables, eran los fenómenos más trascendentales de aquellos días, también se trataba de obligar a las instituciones del Estado a sujetarse a una estricta separación entre intereses de investigación y las tareas que específicamente les había autorizado la ley, así como la obligación de sujetarse a los fines expresados por la ley para el tratamiento de los datos. El control institucional, resumido en la supervisión constante de los Comisionados de la Protección de Datos (Datenschutzbeauftragten), era otro elemento esencial del proceso de nivelación de la legislación a los requerimientos constitucionales establecidos por el Tribunal Constitucional Alemán. Pero también lo era lograr un adecuado desarrollo normativo en todas aquellas áreas que involucraran el procesamiento de datos personales, junto al desarrollo de Comisionados de la Protección de Datos en las propias instituciones públicas y privadas.

Hoy la protección de datos se encuentra viviendo un proceso muy interesante de reformas, algunas de ellas han permitido el desarrollo internacional de las disposiciones de tutela.

Por ejemplo, la Ley Federal de Protección de Datos de Alemania (Bundesdatenschutzgesetz) ya ha incluido dentro de sus disposiciones algunos principios largamente acariciados por los expertos y los ciudadanos como el principio de evitación de datos (Datenvermeidung) y de ahorro de datos (Datensparsamkeit), que no son otra cosa que la aplicación en la práctica del principio de proporcionalidad en esta materia, concretamente del sub principio de necesidad.

La BDSG ha incluido también la llamada auditoría de protección de datos (Datenaudit), que no es más que una regulación complementaria a las ya establecidas de orden institucional y que persigue que haya auditorías llevadas a cabo por expertos particulares, quienes observen en los sistemas la efectiva realización de los principios

[19] Simitis, Konsequenzen, p. 21.

vigentes en la materia. Todos estos cambios han sido bien recibidos por los Comisionados de la Protección de datos[20], quienes las observan como pasos decididos hacia una modernización del estándar de la protección de datos en Alemania y también en Europa, cuyos lemas de campaña son: "protección de datos por medio de la técnica", y "mayor transparencia del procesamiento de datos"[21].

La Unión Europea ha avanzado hasta poner en vigencia una reglamentación sobre protección de datos, y lo mismo ha sucedido en la famosa "Carta de la Unión Europea" que ha reservado un lugar privilegiado para la autodeterminación informativa. Debe distinguirse esta reglamentación de la así denominada "Línea Directiva de la Unión Europea en materia de protección de datos"[22], la cual en realidad se refiere a temas que deben ser puestos en vigencia por los estados miembros de la Unión, así como por los órganos e instituciones de la Unión Europea.

La reglamentación a la que se ha hecho referencia tiene por objetivo proteger a las personas objeto de tratamiento de datos por parte de órganos e instituciones de la Unión Europea. Contiene entre otras regulaciones, la prohibición para órganos e instituciones de la Unión Europea de enviar datos personales a países fuera del ámbito de vigencia de esta reglamentación que no tengan un estándar de protección similar al europeo[23].

Los datos sobre temas sensibles, como el origen o las convicciones religiosas de las personas solo pueden ser tratados de manera automática en casos excepcionales.

---

[20] Ver por ejemplo la Resolución al respecto emitida por los Comisionados de Protección de Datos de Alemania del 10 de octubre del 2000.

[21] Quinto Informe del Comisionado de la Protección de Datos de Mecklenburg-Baja Pomerania, p. 29.

[22] Directiva del Parlamento Europeo y del Consejo sobre la Protección de personas físicas frente al procesamiento de sus datos personales y el libre tránsito de datos del 20 de febrero de 1995. Cfr. Dammann/Simitis, BDSG mit Landesgesetzen, pp. 246 y ss. La versión en alemán puede consultarse en una versión inoficial en: http://www.bfd.bund.de/europa/EU_richtl_de.html

[23] La Ley de Protección de Datos de Inglaterra (UK Data Protection Act de 1998, Schedule 1, Part. 1, Section 8) incluye una norma similar: "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data".

También contempla regulaciones sobre el aseguramiento técnico de los datos, los cuales, desgraciadamente, deben contemplarse como superados, no obstante, la importancia de considerar este tema en la misma reglamentación[24].

Otros aspectos interesantes de esta normativa lo son: la inclusión de un Comisionado de la Protección de Datos, quien, entre otras funciones, le corresponde velar por el cumplimiento de la reglamentación a lo interno de la oficina a su cargo. Junto a este Comisionado, se ha decidido nombrar una autoridad de control constituida por el Comisionado Europeo de la Protección de Datos, quien aconseja y controla a los órganos e instituciones de la Unión Europea en esta materia. Para cumplir con esta tarea se le conceden amplios poderes de acceso a todas las oficinas y centros de procesamiento, a todos los datos personales y a todas las informaciones generadas en el ámbito de la Unión. Contra las decisiones de este alto Comisionado solo se puede iniciar demanda ante el Tribunal Europeo.

Las personas afectadas por procesamientos de datos prohibidos en el ámbito de la Unión, tienen derecho a solicitar información, a obstruir datos y a solicitar y lograr el borrado de datos e informaciones que le afecten. También pueden acudir directamente ante el Comisionado Europeo.

Más importante que lo anterior es que el ejercicio de los derechos que contempla la reglamentación no generan costos para el afectado, lo que indica que esta reglamentación es mucho más amigable con el ciudadano afectado que la misma Línea Directiva del Consejo de Europa[25], la cual indica que las normativas que se dicten bajo la mencionada Directiva no deben incluir costos que sean "exagerados" para el afectado.

Finalmente, la Carta de Derechos Fundamentales de la Unión Europea, que fuera anunciada el día 7 de diciembre de 2000 en Niza, contiene un artículo 8, el cual regula detalladamente aspectos relacionados con la protección de datos, siguiendo muy de cerca la normativa alemana, el texto reza:

---

[24] Quinto Informe del Comisionado de la Protección de Datos de Mecklenburg-Baja Pomerania, p. 30. Están superados si se toma en cuenta el nivel de seguridad técnica con el que cuentan algunas leyes de los Länder luego de las reformas posteriores al año 2000, las cuales hemos denominado en este estudio como "Systemdatenschutz".

(1) "Toda persona tiene derecho a la tutela de sus datos personales.
(2) Estos datos solo deben ser procesados de buena fe para el fin preestablecido con el consentimiento de la persona afectada o para cumplir con los fines establecidos con un adecuado fundamento legal. Toda persona tiene el derecho a recibir información sobre los datos referidos a su persona que hayan sido recogidos y a lograr su rectificación.
(3) El cumplimiento de estas reglas será vigilada por un centro independiente."

El artículo 42 de la Carta garantiza, adicionalmente, un derecho de acceso a los documentos del Parlamento Europeo, del Consejo y de la Comisión.

Aun cuando la Carta no tiene un efecto jurídico directo en la práctica, si es una fuente de interpretación para los órganos e instituciones de la Unión Europea, y objeto de aplicación jurídica y estudio por parte del Tribunal Europeo. En todo caso se nota el alto nivel que se le ha concedido al derecho de la protección datos al nivel europeo, aspecto que terminará por trasladarse a los Estados miembros y a los países que vayan a tener una relación económica directa con la Unión Europea, como puede ser el caso de nuestro país.

Dados los cambios que se han venido produciendo, y la posibilidad de evaluar tres tipos de modelos regulatorios en el horizonte de proyección de esta materia, es que resulta interesante analizarlos, con el fin de contextualizar la reforma propuesta en Costa Rica con el Proyecto bajo examen. A ello dedicaremos la sección siguiente.

4. Diversos Modelos de Regulación

a. La opción hacia la constitucionalización del derecho a la autodeterminación informativa

[25] Al respecto, cfr. Quinto Informe del Comisionado de la Protección de Datos de Mecklenburg-Baja Pomerania, p. 31.

La crisis del concepto de intimidad y las limitaciones que ofrece la tradicional consideración constitucional de la intimidad, han llevado a la necesidad de producir esquemas legislativos que ofrezcan opciones al ciudadano para proteger sus derechos constitucionales, muy especialmente su derecho a la autodeterminación. Fue así como se promulgó la Ley de Protección de Datos del Estado de Hesse en Alemania, que ostenta el honor de ser la primera ley emitida en el mundo para garantizar al ciudadano este derecho.

Otros países han preferido "constitucionalizar" el derecho de acceso a los datos personales. Ejemplos de esta tendencia los encontramos en Colombia y Brasil, también Paraguay en la Constitución de 1992 (art. 136) y Ecuador en la Constitución del 18 de junio de 1996[26]; y en Argentina la Constitución de las Provincias de Jujuy, La Rioja, San Juan; Córdoba; San Luis; Río Negro, Tierra del Fuego y Buenos Aires han incorporado cláusulas referidas a la informática y a la protección de la intimidad. La Constitución de la República de Argentina de 1994 ha establecido la acción de amparo para „...conocer los datos a ella referidos, así como su finalidad, contenidos en registros públicos y privados, y en caso de ser ellos falsos o discriminatorios, exigir su supresión, rectificación, actualización y confidencialidad".

En la República Federal de Alemania, la mayoría de las Constituciones de los Länder o Estados han incorporado el derecho a la autodeterminación informativa como uno más en el elenco de derechos fundamentales.

El debate sobre la necesidad de la constitucionalización sigue vigente en Alemania y en otros países, y los ecos de esta discusión han llegado hasta el ámbito de la Unión Europea. Las voces a favor indican la necesidad de darle un adecuado rango constitucional a este derecho, que supera, en mucho la tradicional tutela ofrecida por la intimidad en su versión tradicional.

---

[26] Artículo 30 de la Constitución de la República de Ecuador, Ley No. 000. R0/969 de 18 de junio de 1996. „Toda Persona tiene derecho a acceder a los documentos, bancos de datos e informes que sobre si misma o sobre sus bienes consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su finalidad.
Igualmente podrá solicitar ante funcionario o juez competente la actualización, rectificación, eliminación o anulación de aquellas si fueran erróneas o afectaren ilegítimamente sus derechos.
Se exceptúan los documentos reservados por razones de seguridad nacional".

Las voces en contra indican que la inclusión del derecho a la autodeterminación informativa es innecesaria, y que basta con los avances legislativos hechos en campos especiales para contar con una tutela completa.

La verdad que el debate parece tener interés en los países que no tienen todavía una tutela legal y específica sobre el tratamiento de datos personales y pueden disponer de tiempo para lograr una adecuada conexión entre las disposiciones constitucionales y la regulación legislativa. Esto significa, por supuesto, que existe la posibilidad -en un corto período de tiempo- de incluir este derecho en la Constitución Política y de contar con un plazo adecuado para poner en vigencia una reglamentación específica para regular los muchos campos en que tiene incidencia la protección de datos. Este último supuesto no suele ser alcanzable en muchos países y pone en peligro tanto el objetivo de alcanzar un estándar normativo aceptable y la meta de una adecuada implementación de las normas de tutela en la práctica. Por esto, constitucionalizar el derecho a la autodeterminación informativa siempre es un primer paso, no siempre necesario, y que requiere de una actividad posterior del legislador conducente a crear las condiciones, en un plano normativo, para lograr un adecuado control del tratamiento de datos, lo que no deja de tener problemas, como podremos observar si tomamos en cuenta la evolución de las leyes en la materia, aspecto que intentaremos analizar en detalle en la sección siguiente.

b. Las generaciones de leyes sobre protección de datos

Con Simitis[27] podemos indicar que ha habido tres generaciones de leyes de protección de datos en el marco del desarrollo histórico de esta área.

La primera generación de leyes se inicia con la puesta en vigencia de la Ley de Protección de Datos del Land Hesse de 1970 y se asienta con la promulgación de la Ley Sueca de 1973. Luego de estos pilares fundamentales, se continúa con la legislación más detallada sobre procesamiento de datos de 1977 en Alemania , así como la Ley de los Estados Unidos sobre privacidad (US Privacy Act) de 1974, y el Privacy Committee

[27] Simitis y otros, BDSG, Parágrafo 1, No. m. 108

Act de la provincia australiana de New South Wales de 1975. Canadá continuaría esta tendencia con el Human Rights Act de 1977, y el hilo conductor se extiende hasta la ley francesa sobre el procesamiento electrónico de datos y de derechos a la libertad de 1978, uniéndose después a este elenco de países Noruega, Austria y Luxemburgo con diversas leyes, finalizando el periodo con la Convención sobre Protección de Datos del Parlamento Europeo de 1981[28].

Todas estas leyes participaban, como lo explicita Simitis, de una misma característica: se trata de leyes que no contaban con una base de casos previamente conocida, así como tampoco de experiencias concretas en la praxis de tutela, por lo que la tarea del legislador era un tanto experimental y confiada a una normativa especialmente flexible, que pudiera irse adaptando a la creciente complejidad tecnológica planteada por la materia bajo examen[29].

La segunda etapa de la legislación de tutela sobre protección de datos se extiende hasta 1988. El periodo se ve caracterizado por la fuerte impresión que dejó la Convención del Parlamento Europeo sobre la protección de la persona frente al tratamiento de sus datos personales de 1981. Las leyes previas a ese año, como la de Islandia, Israel harían sentir el efecto del estándar regulatorio de la legislación sobrevenida a partir de 1981. Luego de ello se pondrían en vigencia un amplio elenco de normativas como la finesa de 1987, la irlandesa también de 1987, el Privacy Act de Australia y la ley japonesa de protección frente al tratamiento automático de datos personales realizado por oficinas públicas de 1988. La ley portuguesa es de 1991 pero aun ella hace denotar una fuerte influencia de la Convención Europea de 1981[30].

Como bien lo expresa Simitis, una evaluación de la ley portuguesa, así como de la israelí y la británica, permite observar como la Convención trascendió con su estándar regulatorio, haciendo que los países asumieran una serie de principios para el tratamiento de datos personales pero con un déficit importante al no permitir una directa intervención en las diversas fases del tratamiento de datos[31].

[28] Simitis y otros, BDSG, Parágrafo 1, No. m. 108
[29] Simitis y otros, BDSG, Parágrafo 1, No. m. 109-113
[30] Simitis y otros, BDSG, Parágrafo 1, No. m. 114

La tercera fase se da en los años ochenta, con la revisión de los principios regulatorios iniciales[32]. El resultado de esta revisión iba a ser muy claro: con ninguno de los modelos anteriores iba a ser posible alcanzar condiciones adecuadas para controlar el tratamiento de datos personales y lograr, al mismo tiempo, un verdadero control preventivo[33]. Esto es especialmente cierto en el modelo de licenciamiento que implicaba, entre otras cosas, un exceso de burocracia con muy escaso éxito en la regulación práctica. En Gran Bretaña, por ejemplo, la exigencia de licenciamiento llevó a crear un registro altamente formalizado[34].

Tampoco el sistema de cláusulas generales (Generalklausen), es decir, reglas que permiten una alta flexibilización, pueden considerarse un modelo aceptable debido, principalmente, a que no siempre permiten llevar el ritmo de los constantes cambios tecnológicos, como tampoco son un límite real para ciertas prácticas o deseos de tratamiento de datos, convirtiéndose más bien en verdaderas formas de legitimación de ciertas prácticas como también de nuevos deseos de procesamiento de datos[35]. Al ser tan flexibles permitían muchas interpretaciones que conducían, en última instancia, a autorizar lo solicitado por el lugar de procesamiento, a quien se le dejaba también la posibilidad de definir los diversos acentos que habría de darse a las interpretaciones[36].

La experiencia derivada de regulaciones específicas en los campos diversos de procesamiento (Bereichsspezifische Regelungsmodell) no permite tampoco ser optimista sobre las posibilidades de éxito, esto último debido, entre otras circunstancias, a las evidentes contradicciones existentes entre las normativas creadas para específicos sectores, como también a la forma sencilla en que los diferentes interesados en el tratamiento de datos logran sus objetivos a la hora en que la regulación específica se dicta[37]. Un claro ejemplo de esto último puede encontrarse en las normativas en el ámbito de seguridad en Alemania[38].

---

[31] Simitis y otros, BDSG, Parágrafo 1, No. m. 114-115
[32] Simitis y otros, BDSG, Parágrafo 1, No. m. 116
[33] Simitis y otros, BDSG, Parágrafo 1, No. m. 116
[34] Simitis y otros, BDSG, Parágrafo 1, No. m. 116
[35] Simitis y otros, BDSG, Parágrafo 1, No. m. 116
[36] Simitis y otros, BDSG, Parágrafo 1, No. m. 116
[37] Simitis y otros, BDSG, Parágrafo 1, No. m. 116
[38] Al respecto Weichert, Gefangen.

En todo caso, y como bien lo subraya Simitis, ninguna de las leyes surgidas en la década de los setenta del pasado siglo podría constituir por sí misma la "única" forma correcta de resolver el problema de derecho planteado por el creciente desarrollo de las tecnologías. Cada una de ellas es hija de su tiempo y responde a las circunstancias en las que surgieron.

La correcta posición sobre el tema más bien sería observar las oportunidades de aprendizaje planteadas por los retos mismos derivados de las tecnologías de la comunicación y la información. Precisamente en esta lógica es que las nuevas leyes que han venido produciéndose en el último tiempo han tratado de enriquecer, por ejemplo, el papel de las instancias de control, y han procurado darle a los Comisionados de Protección cada vez más derechos, con el fin de que éstos velen por la realización práctica de los principios que informan la protección de datos y que son el "núcleo duro" dentro del cual aun se mueve el proceso de reforma[39].

Otros aspectos interesantes en este proceso de aprendizaje lo han sido, sin duda, las diversas experiencias de los países sobre la regulación planteada a partir de la forma del procesamiento, tanto manual como electrónica (lo que plantea la cuestión de cuándo se está en presencia de una u otra), y la difícil cuestión de dar alguna respuesta a la pregunta de si ciertos datos personales pueden o no tratarse, es decir, en concreto, la referencia a los caracteres que permiten definir cuando un dato es sensible o no[40].

En todo caso, estas leyes demostraron ser esenciales como complemento de las garantías generales del Estado de Derecho. Permiten un control no sólo de los así denominados centros de procesamientos públicos, sino también de los privados, garantizando al mismo tiempo derechos a recibir información, a borrar o obstruir el uso de datos que afecten el derecho del ciudadano a saber quién, cuándo y bajo qué circunstancias tiene acceso a sus datos personales[41].

---

[39] Sobre los principios involucrados en la protección de datos y su importancia en el proceso de reforma costarricense, cfr. Chirino, Autodeterminación, pp. 42 y ss.
[40] Simitis y otros, BDSG, Parágrafo 1, No. m. 119
[41] Por ejemplo, dichos derechos se contemplan en el parágrafo 35 de la Bundesdatenschutzgesetz, del 20 de Diciembre 1990, BGBl. p. 2954.

c. El problema de la tutela desde una perspectiva del derecho a la intimidad

El concepto tradicional de intimidad se halla en una crisis evidente[42]. Ya no es posible mantener una tutela basada en los conceptos deciminónicos y burgueses de la intimidad, sino que es necesario dar algunos pasos y comprender el grado de contaminación que ha sufrido este derecho producto del desarrollo tecnológico.

Las sociedades modernas se encuentran ante el dilema de proteger la intimidad en su versión patrimonialista, pero al mismo tiempo deben crear condiciones para mejorar la comunicación de los ciudadanos, así como su autodeterminación. Tienen que velar por un mayor intercambio de informaciones y hacer transparentes muchos usos de la información, y al mismo tiempo garantizar realmente la privacidad de muchos ciudadanos afectados por dichas políticas. Estos dilemas enfrentan a las sociedades modernas ante una complicadísima y difícil ponderación de intereses, donde entran en juego no sólo las necesidades de información de la sociedad, y la nueva configuración de las relaciones económicas entre los países.

Así las cosas, no puede continuarse con un enfoque tradicional en la forma de protección de la intimidad, limitándola a proteger los papeles privados y las comunicaciones telefónicas y telegráficas de los ciudadanos, sino que debe ser considerada en una nueva dimensión: la dimensión de tutela de las posibilidades de participación reales del ciudadano en una sociedad que se informatiza. Esta nueva dimensión de la intimidad se manifiesta, entonces, con un nuevo vestido, el vestido de la autodeterminación y de las facultades de control que un ciudadano debe tener sobre el flujo de informaciones que circulan sobre sí mismo. Este derecho, como lo ha sostenido la doctrina, se vincula no sólo con la intimidad, sino también con derechos constitucionales de gran valor como la dignidad humana, la libertad individual, la autodeterminación y el principio democrático, que antes de ser utilizados como puntos de sustentación vacíos y sin contenido, adquieren una nueva perspectiva en el Estado de Derecho.

---

[42] Cfr., con más detalles: Chirino Sánchez, Eric Alfredo, Autodeterminación Informativa y Estado de Derecho en la Sociedad Tecnológica, San José, CONAMAJ1997, pp. 16 y ss., en el mismo sentido, y planteando la cuestión en el contexto español: Romeo Casabona, Carlos María, Tendencias actuales sobre las formas de protección jurídica antes las nuevas tecnologías, en: Revista del Poder Judicial de España, No 31, Septiembre 1993, pp. 163-204.

Se trata de brindar nuevas condiciones de participación social a los individuos, pero, al mismo tiempo, asegurarles el resguardo de su autodeterminación. Como bien lo postula un Comisionado de la Protección de Datos de Alemania: "La protección de los datos es un presupuesto funcional de la sociedad de la información organizada bajo los supuestos de una sociedad de mercado que desea satisfacer las exigencias democráticas y de derechos civiles. El ser humano "no automático" debe ser protegido en un mundo que se automatiza"[43] .

d. El "Systemdatenschutz" y los enfoques organizativos

Luego de largo tiempo de operar con leyes específicas sobre protección de datos, hubo un movimiento bastante fuerte por reorganizar la forma de tutela de los ciudadanos frente al procesamiento de sus datos personales. La línea común objetiva de este cambio puede definirse como la "protección de datos en una visión de sistema" o "Systemdatenschutz".

Las condiciones de este nuevo paradigma pueden resumirse en las siguientes características[44]:

- Todo procesamiento automático de datos debe contemplar su objetivo concreto así como sus fundamentos jurídicos, de tal manera que puedan reconocerse, fácilmente, los usos antijurídicos de información.
- Deben concebirse conceptos de seguridad que tomen en cuenta las condiciones personales y organizatorias disponibles, de tal manera que se le impida a personas no autorizadas el acceso a dispositivos de almacenamiento de información, en donde se encuentren grabados datos personales. De esta manera se pretende evitar que dichos datos lleguen a

[43] Dronsch, Gerhard, Nochmals: Datenschutz in der Informationsgesellschaft, ZRP, 1996, pp. 206 ss.
[44] La descripción de estos requerimientos han sido tomados directamente de las notas incluidas en el 20. Tätigkeitsbericht (2001) des Ubabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, en: http://www.datenschutzzentrum.de/material/tb/tb23/kap7.htm , donde se detallan los principales aspectos de seguridad incluidos en la reforma a la Ley de Protección de Datos de Schleswig-Holstein, principalmente a los parágrafos 5 al 7 de la Ley del 2000, así como en los parágrafos 3 al 8 de la Datenschutzverordnung (DSVO).

manos no autorizadas y puedan ser procesados afectando a las personas a las que hacen referencia. También se pretende con este tipo de medidas tener claridad de la amplitud del procesamientos de datos, así como de la dimensión temporal dentro de la cual se realiza.

- El uso de sistemas técnicos de información solamente puede ser autorizado una vez que el usuario de turno demuestre su condición de tal (normalmente esto se demuestra una vez que la palabra clave ha sido autorizada mediante un procedimiento de autenticación automática).
- El derecho a intervenir a nivel del sistema solamente puede ser concedido a un número limitado de personas (nivel de administrador). A estos administradores se les debe llevar un control personalizado así como una protocolización de sus intervenciones en el sistema.
- Todo tipo de acumulación de datos que se encuentre grabada en dispositivos de almacenamiento, y que deba ser mantenida fuera del ámbito de seguridad de un lugar de procesamiento, tal y como sucede en supuestos de "teletrabajo" o en el servicio exterior, deben ser encriptados, principalmente con el fin de evitar los daños que podrían ocasionarse a los afectados en caso de un robo.
- Si los datos deben ser grabados exclusivamente de manera electrónica, entonces debe llevarse un control en los registros magnéticos mismos (ante la ausencia de respaldos en papel) de los cambios que se hayan hecho a las informaciones así como de las personas que los realizaron.
- Todos los componentes de hardware y software que son utilizados en un lugar de procesamiento deben ser adecuadamente registrados, con el fin de que se pueda reconocer cualquier tipo de componente ilegal: todo aquello que no esté registrado debe ser desactivado.
- Deben protocolizarse tanto las personas que tienen acceso, así como desde cuando y qué tipo de derechos de uso han tenido a qué parte del hardware o de los componentes de software del sistema, a fin de que puedan ser corroborados mediante comparación con los datos que hayan colocado los responsables del acceso.
- El procesamiento automático debe ser probado acorde con su "uso real" y debe ser puesto a disposición por los encargados del sistema. Con el

fin de lograr esto es que deben ser documentado su uso de tal manera que sea comprensible para un experto en un tiempo razonable.

- El "uso real" del proceso automático debe ser vigilado de tal manera que se determine si las instrucciones de la dirección están apegadas a las disposiciones vigentes. Toda desviación de las autorizaciones para el procesamiento deben ser corregidas.

Hubo reacciones muy diversas de las personas encargadas del desarrollo de software, así como administradores de centros de cómputo, usuarios y otros expertos del campo. Mientras algunos consideraban que por fin el legislador había comprendido el verdadero sentido del concepto de seguridad en el tratamiento de datos, otros no fueron tan optimistas.

En realidad, el problema de fondo radica en que las actitudes frente a bancos de datos manuales son bastante claras: los expedientes suelen ser conservados en un solo lugar, y suelen ser completados con toda la información que les pertenece. Las personas que tienen acceso a él están predeterminadas y se suele llevar un control de aquellos que son autorizados a tener acceso. Lo mismo se estipula sobre archivos de respaldo. No obstante, no puede esperarse que estos viejos principios del manejo de archivos se mantengan siempre cuando los funcionarios tengan acceso a herramientas de procesamiento de datos, en máquinas individuales a su completa disposición y con acceso a los datos almacenados en sus propios discos duros o en cualquier otro medio de almacenamiento, tanto magnético como óptico. Estos usos, accesos y procesamientos individuales pueden llevar a una situación caótica y sin control, que puede hacer que muchas personas se vean afectadas. Por ello es que las decisiones del legislador fueron bien dirigidas y apretaron clavijas donde era necesario, estableciendo una serie de reglas específicas sobre el acceso a la información y al tipo de tratamiento que se le puede dar a un banco de datos por un grupo de personas en un lugar específico de procesamiento, tanto fuera del lugar como dentro de él[45].

[45] Cfr. 20. Tätigkeitsbericht (2001) des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, en: http://www.datenschutzzentrum.de/material/tb/tb23/kap7.htm

El Systemdatenschutz, más que un principio regulatorio, es un instrumento adicional para garantizar seguridad en el tratamiento de datos personal. Su desarrollo no depende directamente de la normativa, sino de la actitud individual de los lugares de tratamiento, por ello, puede verse como una desiderata conducente a crear mejores condiciones para el procesamiento de datos personales.

f. El sistema norteamericano de protección de datos

El sistema norteamericano de protección de datos es diametralmente opuesto al modelo europeo. No sólo no han seguido el camino de dictar leyes específicas en la materia, sino que también han preferido un sistema autoregulado, especialmente desde el punto de vista del derecho del consumidor: los productores deben dar publicidad a sus políticas de privacidad y de cómo las pondrán a punto, con el fin de que los consumidores puedan escoger el que ofrezca un mejor nivel de tutela[46].

En todo caso esta orientación a un sistema autoregulado ha representado para los Estados Unidos un verdadero problema en sus conversaciones con la Unión Europea de cara a acuerdos de libre comercio entre ambos. Los europeos necesitan algo más que la promesa de la autoregulación, tal y como ya lo hemos visto.

La Directiva de la Unión Europea sobre Protección de Datos de 1998 planteó ya los primeros problemas al gobierno norteamericano, quien tuvo que negociar una especie de acuerdo sobre un "puerto seguro" (Safe Harbor)[47] mejorando las condiciones de "funcionamiento" de la tutela de la privacidad en Estados Unidos.

La idea planteada por el Gobierno norteamericano era ofrecer que las compañías norteamericanas aceptarían, libremente, adaptar sus políticas a los principios[48] del "Safe Harbour", que no son otros que simples reconstrucciones a los principios contenidos en la Directiva de la Unión Europea de 1995 a la que ya hemos hecho referencia antes.

---

[46] Kirsh/Philips/McIntyre, Recommendations for the evolution of Netlaw: Protecting Privacy in a Digital Age, en: Jorunal of Computer-Mediated Communication, en: http://jcmc.mscc.huji.ac.il/vol2/issue2/kirsh.html

[47] Más información al respecto puede ser consultada directamente en: http://www.export.gov/safeharbor/

[48] Una explicación de estos principios y su significación puede ser consultada en la página propuesta por el Departamento de Comercio de los E.E.U.U. http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm

Entre ellos, por ejemplo, que las compañías estadounidenses se comprometen a que la información sólo será utilizada para los propósitos para la cual fue recogida. Además, proveerán información a los clientes sobre la posibilidad de acceso a la información, proveyéndolos de condiciones para que puedan corregir discrepancias y datos inexactos en los bancos de datos que las empresas hayan puesto en funcionamiento. También se establecerán políticas sobre seguridad de los datos, además de información al cliente sobre el hecho de que sus datos personales están siendo procesados.

La propuesta de "safe harbour" planteada por el Departamento de Comercio de los Estados Unidos fue admitida por la Comisión Europea en julio del año 2000, como un ejemplo de adaptación a los principios de la Directiva del año 1998, aun cuando puede coincidirse con Guadamuz que dicha aceptación no es más que una cesión en virtud de los poderosos intereses económicos involucrados[49].

g. La respuesta latinoamericana: el habeas data

En la literatura latinoamericana es recurrente la referencia al habeas data, como forma de tutela de los ciudadanos frente al tratamiento de sus datos personales.

La vinculación del habeas data con el habeas corpus es mucho más que casual, y puede encontrarse literatura que defiende un concepto de “habeas data” como una acción similar al habeas corpus[50], esto es, que en lugar de “traer el cuerpo”, se trata de “traer los datos”. Qué se hará con ellos y qué amplitud de tutela se ofrecerá dependerá, en casi todos los casos de la regulación normativa específica o de la interpretación que den los Tribunales, usualmente constitucionales, a la cuestión.

---

[49] Cfr. Guadamuz, Andres, Habeas Data: The Latin-America Response to Data Protection, en: http://elj.warwick.ac.uk/jilt/00-2/guadamuz.html

[50] Sagués, Néstor Pedro, El Habeas Data: Alcances y Problemática, en: Sánchez, Alberto, El derecho público actual. Homenaje al Prof. Dr. Pablo A. Ramella, Buenos Aires, Depalma, 1994, p. 179, cfr. También Chiriboga Zambrano, Galo, La acción de amparo y de hábeas data: garantías de los derechos constitucionales y su nueva realidad jurídica, en: http://www.ildis.org.ec/amparo/hab.htm .

Suele vincularse a su núcleo de tutela los derechos a la honra, a la buena reputación, a la intimidad y al derecho a informarse[51].

En la discusión del problema del procesamiento de datos en América Latina surge casi por asociación inmediata el concepto de „habeas data“. Derivado en gran medida del concepto de „habeas corpus“, el habeas data pretende hacer referencia a la posibilidad jurídica de proteger el derecho de los ciudadanos a acceder a las informaciones personales que se encuentren disponibles en registros magnéticos y manuales con el fin de ser revisados, y si representan para la persona un perjuicio, también el de ser corregidos o eliminados.

Debe insistirse que no se trata de un derecho del ciudadano a poseer los datos, ni tampoco de exigirlos como si se tratara de un ejercicio derivado del derecho a la propiedad. Se trata más bien de instrumentar una verdadera garantía procedimiental para que realice un derecho sustantivo que a su vez intenta proteger el derecho del ciudadano a saber quién, cuándo, con qué fines y en qué circunstancias toma contacto con sus datos personales. Esta articulación suele ser difícil, ya que el habeas data no es más que una garantía procedimental, esto es una garantía para acudir a una determinada vía y ahí solicitar los datos o las informaciones que se entiende son lesivas a los derechos protegidos, y como pretensión solicitar la anulación, borrado, obstrucción o corrección de los datos que afectan a la persona. Se trata, entonces, de un derecho reactivo y no de uno preventivo. Funciona cuando ya ha sucedido un daño, que puede ser, en algunos casos de incalculables proporciones, por la afectación que puede recibir una persona al producirse interconexiones automáticas de los bancos de datos

Concebir al habeas data como un derecho absoluto sobre los datos o un medio procesal para ejercer un poder “cuasi” patrimonial sobre ellos, sería incorrecto. Tan incorrecto, como concebir a la autodeterminación informativa como otra forma para el derecho a poseer los datos. El derecho a la autodeterminación informativa no le concede al

[51] Así, por ejemplo, Chiriboga, La Acción, op. Cit. La Constitución Federal Brasileña considera incluidos dentro del ámbito de tutela del habeas data, tanto a la vida privada, a la honra, el derecho a la imagen, y concentra el ámbito e tutela a las informaciones contenidas en bancos de datos pertenecientes a entidades públicas o de carácter público, lo que está previsto en el Art. 5º, LXXII de la actual Carta Magna brasileña

ciudadano un definitivo y absoluto poder sobre sus datos[52], sino el derecho a estar informado del procesamiento de los datos y de los fines que se pretende alcanzar, junto con los derechos de acceso, corrección o eliminación en caso de que se cause un perjuicio. Aquí se pone el interés, entonces, en la „autodecisión“ o en la „autodeterminación“ del individuo, lo que se desea es garantizarle su posibilidad de participación como ciudadano frente a un procesamiento de datos personales que lo puede hacer transparente para el control y reducirlo a un mero objeto del ambiente informativo.

Desgraciadamente, el habeas data latinoamericano se ha concentrado en un derecho reactivo de índole procesal constitucional[53], y decimos desgraciadamente, porque ha hecho que la figura dependa de la amplitud y generosidad de la interpretación de los tribunales constitucionales de los diversos supuestos o constelaciones de casos. Los modelos europeos y norteamericanos se inspiran en diversos puntos de partida. En el caso europeo, como ya hemos visto, se ha puesto el acento en establecer deberes, la mayor parte de ellos preventivos, para salvaguardar a la persona antes de que sucede a una posible afectación a su derecho a la autodeterminación informativa. Los Estados Unidos han preferido tutelar acciones individuales bajo el amparo de una ley que defiende específicamente la privacidad de los hogares y de las personas[54].

El habeas data, en nuestra concepción, se queda a medio camino, entre la tutela integral de los ámbitos de autodeterminación del ser humano, y la posibilidad de construir una tutela preventiva de las lesiones que como inmensos riesgos se ciernen sobre las posiciones jurídicas de los ciudadanos en una sociedad orientada a la información. No debe dejarse de lado, que los derechos de la tercera generación[55], en la clasificación de

[52]Scholz, Rupert y Pitschas, Rainer, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, Berlin, Dunker und Humblot, 1984, p. 27.

[53] Sobre el carácter indudablemente constitucional del habeas data cfr. en lugar de muchos otros: Gozaini, Osvaldo Alfredo, El proceso de habeas data en la nueva ley, en: http://www.abogarte.com.ar/habeasdata1.html

[54] Así Gozaíni, Proceso, op. Cit.

[55]Las leyes de la primera generación serían, según este autor, las leyes que se concentraban en una autorización previa de los bancos de datos, lo que tenía sentido ya que estas leyes surgieron cuando el procesamiento de datos era centralizado, los equipos voluminosos y fácilmente localizables. Luego surgieron las „leyes de la segunda generación“, las cuales pusieron el énfasis en los datos sensibles, a fin de evitar daños a la privacidad y ofrecer alguna garantía frente a posibles prácticas discriminatorias que pudieran tener su origen en el uso de esos datos „sensibles“. Luego vendrían las leyes de la tercera generación, interesadas en el „uso“ y „funcionalidad“ de las informaciones. Aquí ubica Pérez Luño, por

Pérez Luño, surgen ante el fenómeno inevitable de la "contaminación" provocada por ciertos usos de las nuevas tecnologías[56]. El derecho a la autodeterminación informativa es uno de estos derechos, y exige que la regulación normativa sea coherente con su naturaleza. Es por ello que deben tomarse en cuenta no sólo los derechos de acceso y control, sino también previsiones de carácter técnico que salvaguarden, con efectividad, los derechos involucrados[57].

La inevitable limitación que ofrece una garantía exclusiva en el ámbito procedimental se manifiesta, muy especialmente en Brasil, donde la Constitución misma restringe el ejercicio del habeas data contra incorrectos datos e informaciones contenidos en bancos de datos públicos, lo que es una decisión incorrecta, si se le evalúa, por ejemplo, desde la perspectiva del cambio de posiciones acaecido en la década de los ochenta y noventa del pasado siglo, cuando los privados adquirieron un enorme poder informático y lo utilizaron para vender datos personales y con ello generar un riesgo insospechado para la capacidad de autodeterminación de las personas.

El habeas data poco va a lograr si conserva esa naturaleza de mera garantía procedimental[58], ya que obligará a poner todas las cartas en el ejercicio ex post de la jurisdicción. Sería mucho más práctico avanzar en dirección del reconocimiento de un derecho del ciudadano a desarrollar un plan de vida, de crear las condiciones de su autorrealización en una sociedad de conocimiento. Si el problema se visualiza desde allí, podrá comprenderse que lo que hay de por medio se trata realmente del viejo problema de otorgar un verdadero y efectivo status civitatis a la persona, para que pueda desarrollar su personalidad y definir las condiciones dentro de las cuales interactuará con sus semejantes.

Es por ello, que consideramos que un ejercicio del habeas data, sin un correlativo derecho de información sobre las formas en que se realizará el procesamiento, los

---

ejemplo, a la LORTAD española.. Cfr. Pérez Luño, La Tutela de la Libertad Informática, op. cit., pp. 97-98.

[56] Cfr. Pérez Luño, La Tutela de la Libertad Informática, op. cit., p. 97.

[57] Esta unificación entre herramientas técnicas y protección de datos es promocionada, por ejemplo, por Hassemer, Winfried, Über die Absehbare Zukunft des Daztenschutzes, KJ (Alemania) 1996, pp. 103 y ss.

[58] El art. 5, inciso LXXII de la Constitución brasileña postula: „...ceceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros de bancos de dados de entidades governamentais ou de caráter público; b) para a retificação, quando não se prefira fazê-lo por processo sigiloso judicial ou administrativo".

objetivos y fines del mismo, la extensión, el destino final de los datos personales le quita transparencia, por un lado al procesamiento mismo de los datos y, por el otro, hace imposible que el ser humano tome nota de que sus datos serán objeto de manejos más allá de su decisión, con incalculables consecuencias para él, tanto dentro como fuera de las fronteras de su país.

5. El „Habeas data" como forma de protección de la persona frente al tratamiento de datos personales en Costa Rica

Un proyecto redactado en el año de 1996 intentó introducir una reforma a la vigente Ley de la Jurisdicción Constitucional No. 7135 del 19 de octubre de 1989, a fin de que se adicionara un Capítulo IV referido al „Habeas Data" en el Título III sobre los recursos, como una forma de „amparo específico" en materia de tutela de la „identidad" o „libertad" informáticas[59].

Se partía de la premisa de que el amparo en Costa Rica era lo suficientemente amplio como para brindar una tutela a la libertad informática “sostenible”, haciendo una curiosa separación entre “habeas datas propio" e “impropio", siendo este último el que garantiza el acceso a la información, frente a la cual se tiene un „interés legítimo"[60].

El así llamado „habeas datas propio" contemplaría los derechos de acceso, modificación, adecuación al fin, confidencialidad, eliminación e inclusión de datos de la persona. No se analiza cuáles etapas del tratamiento de la información serían tuteladas, y parece desprenderse de la argumentación de los motivos del Proyecto, que se atiende al interés en cuanto al dato final, tal y como se encuentra consignado en el banco de datos, no así, por ejemplo, a las fases de recogida y grabación de los datos o, por ejemplo, la transmisión de datos más allá de las fronteras.

El Proyecto consideraba necesario contemplar esta figura procesal, con el fin de lograr una ágil y efectiva forma de acceso “acorde con los derechos en peligro".

---

[59] Un análisis detallado de este Proyecto de Ley puede encontrarse en Chirino, Autodeterminación, pp. 21 y ss.
[60] Exposición de Motivos, Expediente No. 12827, p. 30.

En cuanto a los derechos merecedores de tutela a través de esta forma de garantía procedimental se citaban, entre otros la "autodeterminación informativa"[61], la "intimidad" y la „libertad informática", es decir, una serie de contenidos conceptuales abarcadores de otros tantos derechos derivados de la dignidad humana y del libre desarrollo de la personalidad.

Lo que no se entiende, es cómo es que será posible conjurar los peligros de „estigmatización del individuo" y en el "aspecto social", cuando toda la apuesta normativa se concentra a permitir la reacción cuando el daño ya se ocasionó, y las ulteriores consecuencias podrían sentirse, sin exageración, en otras latitudes vía el flujo transfronteras de datos personales, uno de los supuestos más importantes de la "aldea global" en la que se ha convertido nuestro mundo.

Los efectos de una regulación como ésta podrían ubicarla como un intento más de "patrimonializar" la tutela de la intimidad, fenómeno que ya hemos discutido en otra parte[62].

6. Análisis de la jurisprudencia constitucional sobre el habeas data

La Sala Constitucional ha venido realizando, entre tanto, una interpretación del artículo 24 que se concretó, inicialmente, en el concepto de intimidad entendido como un *"...derecho del individuo a tener un sector personal una esfera privada de su vida, inaccesible al público salvo expresa voluntad del interesado"*.[63] Refiere entonces, en una primera instancia, a la difícil discusión de lo que es la "esfera privada de vida". Para intentar delimitar los marcos de esta esfera privada, el analista se encuentra hoy

[61] Exposición de Motivos, Expediente No. 12827, p. 7.
[62] Cfr. Chirino, Alfredo, La tutela de la autodeterminación informativa como un nuevo bien jurídico penalmente tutelado. El caso del Proyecto de Código Penal de Costa Rica de 1995, en: Revista Nueva Doctrina Penal, Buenos Aires, Argentina.
[63] Sala Constitucional, V. 5736-94, citado según Córdoba, Fallas, Ramírez, Valerín, Constitución Política de la República de Costa Rica. Concordada, Anotada y con resoluciones de la Sala Constitucional, San José, Costa Rica, Asamblea Legislativa, 1996, p. 101.

con algunos ejemplos citados por la jurisprudencia, que usualmente conducen a una lectura tradicional de la estructura de la intimidad en la Constitución costarricense de 1949[64], tales como: la inviolabilidad de los documentos e informaciones privadas y el secreto bancario.

La Sala Constitucional costarricense, sin embargo, ha tomado consciencia de otros problemas que tienden a superar el enfoque tradicional de la intimidad, como lo es la dificultad para vivir en una sociedad donde un ciudadano no tiene *"...derecho a mantener reserva sobre ciertas actividades u opiniones suyas y obtener amparo legal para impedir que sean conocidas por otros, en especial cuando para conocerlas deban emplearse procedimientos clandestinos..."*[65] Y esto es así, toda vez que la mención a los procedimientos clandestinos de acceso a la intimidad no sólo abre un frente de batalla contra el control ilegal y los ataques desproporcionados que sufre la intimidad con la acción de los órganos de la investigación criminal, como porque también toma en cuenta que para un ciudadano *"...resulta imposible o muy difícil convivir y desarrollar a plenitud los fines que una persona se propone, sin gozar de un marco de intimidad, protegido de injerencias del Estado y otros ciudadanos"*[66].

En efecto, la intimidad, en su concepto constitucional, no sólo protege la „esfera privada" de los ciudadanos como un área donde se excluye del conocimiento de los otros una serie de datos e informaciones, salvo manifestación expresa del afectado, sino que su salvaguarda garantiza también el desarrollo a plenitud de la persona, la posibilidad de la „convivencia" y, agregaríamos nosotros, la posibilidad de participación activa en el proyecto social, mediante el ejercicio de otros derechos fundamentales.

La intimidad es, entonces, no sólo la salvaguarda de la esfera privada, sino también una garantía de convivencia y participación social. Es una unión de la idea de tutela de una esfera íntima y recóndita, con la idea de libertad en la democracia, y en tal sentido,

---

[64] Esta estructura, que hemos llamado tradicional, ha sido comentada en la investigación titulada: La tutela de la autodeterminación informativa como un nuevo bien jurídico penalmente tutelado, de pronta aparición en la Revista Nueva Doctrina Penal, de la Editorial del Puerto, donde hacemos referencia a los problemas que enfrenta el derecho penal para asumir una tutela moderna de la intimidad, aspecto que tiene mucho que ver con la superación de la estructura tradicional de tutela derivada del derecho constitucional. Cfr. Chirino, La Tutela, op. cit., passim.

[65] Sala Constitucional, V.3308-94 citado según: Córdoba y otros, Constitución Política, op. cit., p. 101.

opera como un punto de entronque con el concepto de autodeterminación informativa, en tanto y en cuanto, se garantice para el ciudadano un derecho de acceso a sus datos personales, como ejercicio activo de su participación democrática[67].

Una observación de los fallos recientes de la Sala Constitucional contribuye a fundamentar nuestro aserto de que la consideración del derecho a la autodeterminación informativa, en su forma de reconocimiento de otras libertades civiles de las personas, es una línea dominante en la jurisprudencia de nuestro Tribunal Constitucional. De hecho, es esperable, tarde o temprano, algún fallo de principio que siente las bases del derecho del ciudadano a ser protegido ampliamente de los riesgos derivados de un tratamiento de datos abusivo y desproporcionado.

a. Aceptación del concepto de autodeterminación informativa en nuestra jurisprudencia constitucional

La Sala Constitucional ha ido evolucionando en su interpretación de la tutela de la intimidad que puede derivarse del artículo 24 de la Carta Magna.

En un fallo que puede definirse como un punto de partida inicial, la Sala estudió este derecho en su forma tradicional con el fin de explorar las posibles limitaciones que pueden ponerse al interés del Estado por intervenir las comunicaciones telefónicas de

---

[66] Ibid.

[67] Como lo señala Podlech, comentando la Ley Fundamental de Bonn de 1949, la protección constitucional de la intimidad tiene una dimensión material, constituida por la protección del libre desarrollo de la personalidad, de la autodeterminación informativa, del respeto al ámbito privado del ciudadano, pero también ostenta una dimensión institucional caracterizada por la protección del matrimonio y la familia; y una dimensión espacial constituida por la protección de la habitación. Es decir, que la intimidad o privacidad no se agota en una sola de esas dimensiones, sino que han de atenderse todas ellas en la protección jurídica, ya que la intimidad tiene, en relación con la democracia una conexión directa. Muchos derechos fundamentales, aquí también la privacidad, ganan su legitimidad precisamente de su capacidad para coadyuvar en el funcionamiento de la democracia. Es por ello que las limitaciones a la privacidad y las limitaciones a ésta que pongan en peligro al ejercicio de derechos fundamentales que forman parte esencial de la participación en la democracia, serían inaceptables en un régimen constitucional democrático. Cfr. Podlech, Adalbert, Das Recht auf Privatheit, en: Perels, Joachim (Edit.), Grundrechte als Fundament der Democratie, Frankfurt am Main, Suhrkamp, 1. Edición, 1979, p. 52.

los ciudadanos con el objetivo de investigar ciertos delitos[68].

Esta línea jurisprudencial sería continuada por una dupla de fallos: el 2609–91 y el 2680–94, donde el problema central era observar si existe algún deber de confidencialidad de los datos que son conservados en acervos creados vía legal, como es el caso de los que ha organizado el Organismo de Investigación Judicial.

En el fallo 2609-91 se trataba de ver, en concreto, si podía entregarse información de la contenida en estos bancos de datos a terceras personas, que no son autoridades públicas, para un fin, además, que no estaba establecido en la ley creadora del archivo (desviación del fin original del tratamiento de datos).

La sentencia 2609-91 es un antecedente contradictorio y esto por dos razones: en primer lugar, la Sala estimó que no era necesario remover una información imprecisa del registro del Organismo de Investigación Judicial, considerando que ningún daño ocasionaría a la persona referenciada en el mismo. Afortunadamente, este criterio se variaría a favor del derecho a la autodeterminación informativa en el Voto 5802-99.

No obstante, la aceptación más directa de la "informationelle Selbstbestimmung" se haría en el fallo 1998–1345 de las 11:36 horas del 27 de febrero de 1998. Este antecedente es importante por muchas razones:

- Fue el primer fallo donde se establecería una relación inequívoca entre los peligros de la "sociedad informatizada" y el derecho a la intimidad.
- Hace un reconocimiento de los riesgos que las tecnologías de la comunicación y la información podrían traer para la sociedad y el ciudadano, sobre todo en lo referido al acceso a los datos personales.
- Se involucra el fallo en la discusión científica sobre los riesgos que representa para los derechos fundamentales un uso indiscriminado de las tecnologías para construir, por ejemplo, perfiles de los ciudadanos, que puedan afectar sus derechos de participación, lo que permite derivar la aceptación del nuevo papel dinámico en el cual debe desenvolverse la interpretación moderna del concepto

[68] Sala Constitucional, 1261–90 de las 15:30 horas del 9 de octubre de 1990 (Intervenciones

de intimidad.

- En cuanto a la necesidad de tutelar a los ciudadanos frente al riesgo de construir personalidades de "cristal", transparentes al control, menciona esta sentencia con claridad meridiana lo siguiente:

> *".... Así ocurre, cuando se desarrollan perfiles de las personas utilizando información aislada y aparentemente inofensiva, como edad, sexo, dirección, educación, estado civil, preferencias, entre otros muchos. En algunas situaciones esta información es factible utilizarla para definir a los "sospechosos" o a aquellos considerados "políticamente inapropiados", lo cual implica, que las personas así catalogadas sean excluidas de un papel activo en la sociedad. La informática, no sólo representa uno de los más grandes avances del presente siglo, sino que pone en evidencia las posibilidades de inspección de la vida interior de las personas, desde este punto de vista, la personalidad de los ciudadanos y su fuero interno cada vez se hacen más trasparentes. Esta situación hace necesario que los derechos fundamentales amplíen también su esfera de protección"*[69].

- Los magistrados constitucionales hacen evidente que la "...esfera privada ya no se puede reducir al domicilio o a las comunicaciones sino que es factible preguntarse si debe incluir "la protección de la información" para reconocerle al ciudadano una tutela a la intimidad que implique la posibilidad de controlar la información que lo pueda afectar[70].
- Insiste en el tratamiento electrónico de datos, pero podemos extender los efectos de este fallo también al tratamiento manual, y que éste debe afianzar los derechos y garantías democráticas del ciudadano, citando una amplia paleta de principios constitucionales derivados de los artículos 24, 1, 28, 30, 33 y 41 de nuestra Carta Fundamental.

Telefónicas).

[69] Sala Constitucional, Sentencia 1998–1345 de las 11:36 horas del 27 de febrero de 1998. (Autodeterminación Informativa)

[70] Sala Constitucional, Sentencia 1998–1345 de las 11:36 horas del 27 de febrero de 1998. (Autodeterminación Informativa)

- La tendencia a visualizar nuevas facetas del derecho a la intimidad en su enfrentamiento a los peligros de la sociedad informatizada queda plasmada en la dicotomía subrayada por los jueces que se presenta entre el desarrollo económico prometido por las nuevas tecnologías y la necesidad de seguir garantizando tutela a los ciudadanos frente a los posibles abusos que se puedan dar, fue así como se argumentó que:

> *"...El nuevo derecho a la intimidad, debe ponderar los intereses en conflicto, entre el legítimo interés de la sociedad a desarrollarse utilizando la información, como la también necesidad de tutelar a la persona frente al uso arbitrario de sus datos personales. La tutela a la intimidad implica, la posibilidad real y efectiva para el ciudadano de saber cuales datos suyos están siendo tratados, con que fines, por cuáles personas, bajo que circunstancias, para que pueda ejercer el control correspondiente sobre la información que se distribuye y que lo afecta (arts. 24 de la Constitución y 13 inciso 1, de la Convención Americana de Derechos Humanos)…"*[71]

Esta importantísima sentencia demuestra que la Sala Constitucional ha decidido entender ampliamente la relación existente entre el derecho a la intimidad y el principio democrático, observándola como un presupuesto esencial para el ejercicio de otros derechos fundamentales previstos en la Constitución de 1949 que definen al ciudadano como una entidad que actúa libre, interactuando con otros y desarrollando su plan de vida libre de intervenciones estatales o privadas, mientras este plan no entre en contradicción con las bases del sistema (Artículo 28, segundo párrafo, de la Constitución de 1949). Se trata de una difícil interpretación, donde los bienes jurídicos en juego, son de difícil equilibrio, como el mismo Tribunal Constitucional lo ha reconocido[72].

[71] Sala Constitucional, Sentencia 1998–1345 de las 11:36 horas del 27 de febrero de 1998. (Autodeterminación Informativa)
[72] Sala Constitucional V.678-91, citado según Córdoba y otros, en: Constitución Política, op. cit., p. 110.

Como anotación final debe subrayarse que la aceptación del vocablo "autodeterminación informativa" tiene una serie de consecuencias de orden constitucional, y por supuesto, significa una toma de posición sobre el bien jurídico tutelado. El concepto de "autodeterminación informativa" (Recht auf informationelle Selbstbestimmung) ha sido incorporado por la doctrina y jurisprudencia alemana, y manifiesta un status interpretativo bastante claro, sin embargo, en el ambiente europeo no parece haber una aceptación de este concepto, cuando, por ejemplo, se prefiere hablar de un "droit à la vie privèe" o de un "right to privacy", que tienen una mayor orientación a la tutela de la vida privada, tal y como está regulada en el artículo 8 de la Declaración Europea de Derechos Humanos. En estos otros ordenamientos jurídicos sigue presente una fuerte impronta por la tutela de la "esfera privada", la que desde nuestro punto de vista tiene serias dificultades para una efectiva comprensión, análisis e interpretación dogmática de los ataques tecnológicos al derecho del ciudadano a determinar quién, cuando, dónde y bajo qué circuntancias toma contacto con sus datos personales. Aspecto este último que parece haber quedado claro para nuestro Tribunal Constitucional.

b. **Las referencias al habeas data en la jurisprudencia constitucional**

La Sala Constitucional ha reconocido la existencia de un “amparo especial”, denominado “habeas data” cuyo objetivo esencial consiste en el ejercicio de una facultad de corrección de los datos que se hallan en bancos de datos públicos y privados.

La primera sentencia que alusión a este tema es la número 4154-97. Califica al habeas data, correctamente, como una institución de carácter procesal, cuya tutela se extiende a bienes jurídicos tales como el honor, la intimidad y la dignidad de la persona.

Para dar entrada a este tipo de pretensiones procesales, acude nuestra Sala Constitucional al artículo 11 del Pacto de San José, cuyos párrafos 1 y 2, que sientan las bases para crear un ámbito de tutela para la honra y la dignidad de los seres humanos, impidiendo que una persona pueda ser objeto de “...injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de

ataques ilegales a su honra o reputación"[73].

De este articulado, desprende la Sala Constitucional, a nuestro modo de ver correctamente, la base fundamental para un derecho genérico al acceso de las personas a su información sensitiva, con el fin de *"...saber qué se dice de la persona en los registros que pueda tener el Estado o los particulares y en el derecho a la rectificación de esa información, que consiste en la facultad de corregir datos inexactos que obren en registros públicos o privados, respecto a la edad, antecedentes, cualidades etc"*[74].

En cuanto al "habeas data", menciona este importante fallo que es una forma o modalidad de "recurso de amparo" cuyo objeto es conocer o rectificar "*...toda la información pública o privada que exista sobre ella, incluso la que no ha sido utilizada ni haya de serlo en su perjuicio..."*[75]

El fallo no deja de lado la referencia a la importancia del tratamiento de datos personales utilizado en el trámite de selección de personal, pero, al mismo tiempo indica, con razón, que: *"..., en caso de que las personas soliciten acceso a la información que sobre ellas se haya recabado, ésta debe ser suministrada. Las pruebas anónimas, para el fin que sean, violan el derecho fundamental a conocer lo que de la persona se dice o los datos que sobre ella se conservan, lo contrario es inadmisible en el sistema democrático y a la luz del Derecho de los Derechos Humanos…"*[76]

Los aspectos sentados por este fallo, fueron reiterados después en el Voto 1997–7175 de las 19:30 horas del 16 de julio de 1997.

c. **¿Habeas data o autodeterminación informativa?**

En el importante Voto N° 2000–3820 de las 10:05 horas del 9 de mayo de 2000, donde se planteó el tema de la negativa del Ministerio de Relaciones Exteriores y Culto de entregar a un periodista del diario "La Nación" una certificación de los expedientes administrativos y pasaportes de dos extranjeros, la Sala volvió sobre el tema del habeas

[73] Artículo 11.2 de la Convención Americana de Derechos Humanos (Pacto de San José) citado por la Sala Constitucional, Sentencia 4154-97, Considerando IV.(Habeas Data)
[74] Sala Constitucional, Sentencia 4154-97, Considerando IV.(Habeas Data)
[75] Sala Constitucional, Sentencia 4154-97, Considerando IV.(Habeas Data)
[76] Sala Constitucional, Sentencia 4154-97, Considerando IV.(Habeas Data)

data y su carácter de garantía procedimental, pero intentando, al mismo tiempo, extender su ámbito de acción para convertirlo en un verdadero instrumento de orientación al tratamiento de datos personales, una interesante variante en la jurisprudencia constitucional en Costa Rica.

En efecto, en este caso, además de señalar la condición de "amparo especial" del habeas data, dice que su objeto lo es los datos e informaciones que se encuentran en bancos o bases de datos. Le concede al ciudadano acceso a todas las "registraciones" que sobre su persona existan, con la finalidad de suprimir, rectificar, modificar o actualizar la información que esté contenida en los mencionados acervos. No obstante, la Sala no se queda en un mero derecho de acceso, sino que introduce un derecho a saber, es decir, a conocer qué informaciones íntimas se encuentran en los bancos de datos y a controlar el uso abusivo de la información íntima contenida. Lo dice prístinamente: "*... Por lo que trata de que una persona evite el uso abusivo de la información que de él se tiene, además de evitar la divulgación de esos datos. Comprende el derecho al acceso, cuando un sujeto está registrado de algún modo en un banco o base de datos, tiene derecho a saber lo que consta acerca de su persona*"[77].

Las facultades de control comienzan con el saber, esto es, con el derecho a la información que la persona tiene. No se puede controlar lo que no se conoce. Por esto, la Sala conecta el derecho a la actualización que tienen los afectados con el derecho a adquirir una verdadera "identidad informática", lo cual explica de la siguiente manera: "*...El Hábeas data se une al concepto de identidad informática, entendida como el conjunto de datos que permiten reconstruir la imagen moral de su personalidad – elementos de orden biológico, predisposiciones a enfermedades hereditarias, malformaciones físicas, condiciones psíquicas, de carácter, temperamento, aptitudes, datos que recogidos, memorizados y elaborados en un computador electrónico, llegan a ser accesibles inmediatamente y difundibles, y aún susceptibles de mercado o venta. El ejercicio del Hábeas data ha sido calificado de ser un mero recurso procedimental de protección de la esfera de la intimidad. De ahí que podría funcionar en caso que el ciudadano considere que su intimidad fue lesionada por un particular o el Estado. Se garantiza la defensa de la intimidad respecto al tratamiento automatizado de datos*

[77] Sala Constitucional, Sentencia 2000–3820 de las 10:05 horas del 9 de mayo de 2000.(Habeas Data como derecho a accesar, controlar y a saber)

personales que se halla garantizada por este cauce procesal. Se concibe a la intimidad como un derecho (status negativo) de defensa frente a cualquier intromisión de la esfera privada, sin contemplarla, al propio tiempo como un derecho activo de control (status positivo) sobre el flujo de informaciones que conciernen a cada sujeto …"[78]

La frase final citada sobre la "intimidad como un derecho (status negativo)" parece, en todo caso contradictoria, con el sentido general de lo resuelto. En efecto, desde nuestra perspectiva si la Sala Constitucional viene delineando la creación de facultades generales de información y control para los ciudadanos, esto no puede ser nunca un status negativus, sino más bien una garantía positiva que reivindican los ciudadanos en el estado de derecho de la sociedad tecnológica. Precisamente, la nueva dimensión del derecho a la intimidad que se proyecta con la "autodeterminación informativa" implica un "status positivus", esto es una verdadera garantía activa del ciudadano para intervenir en el flujo de informaciones, por supuesto, no con una pretensión exclusivamente derivada de un derecho de propiedad, sino con el fin de lograr respeto a sus derechos de autodeterminación, de libre desarrollo de su personalidad, en una palabra, de su dignidad.

Esta desafortunada expresión, fue abandonada en otro de los grandes hitos de nuestra jurisprudencia constitucional. Nos referimos al Voto No. 5802–99 de las 15:36 horas del 27 de julio de 1999. Se trata nada menos y nada más que del primer fallo donde la Sala abordó los principios que regulan el tratamiento de datos personales. Esto es, dio cabida, dentro de la tutela procesal del habeas data, a que el ciudadano pueda controlar la forma en que se realiza el tratamiento de datos personales.

La Sala no sólo reafirma el fértil camino iniciado por el Voto 1998–1345 de las 11:36 horas del 27 de febrero de 1998, en cuanto a reconocer como objeto del habeas data el derecho a la autodeterminación informativa, sino que continúa buscando con intensidad vincular a la intimidad con los derechos constitucionales que garantizan la realización y determinación de la persona, tales como el derecho a la participación política, el derecho a asociación, a la expresión y el libre desarrollo de la personalidad.

[78]Sala Constitucional, Sentencia 2000–3820 de las 10:05 horas del 9 de mayo de 2000.(Habeas Data como derecho a accesar, controlar y a saber)

El derecho a la autodeterminación informativa cobra valor como derecho humano de la tercera generación, tanto en los procesamientos de datos que realiza la administración pública, como también la que realizan los particulares. Esta postura queda ratificada de la siguiente manera, en el fallo bajo examen: *"...Esta tutela resulta necesaria ya que los incesantes cambios tecnológicos ponen en peligro este derecho constitucionalmente consagrado al crear medios para alcanzar perfiles detallados de la personalidad de un ciudadano o ciudadana, que bien pueden convertirlo en un objeto del funcionamiento estatal o de los privados, quienes también poseen en la actualidad medios para alcanzar un control y vigilancia de los ciudadanos en una intensidad desconocida en etapas anteriores del desarrollo de las tecnologías de la comunicación y de la información. Esta objetivización del ciudadano por los medios tecnológicos, para efectos de convertirlo en un ente transparente para cualquier fin estatal, contraría los fundamentos básicos del consenso constitucional de 1949, el cual se basó en un Estado de Derecho de base democrática, tal y como lo establece la conjunción de los artículos 1 y 28, segundo párrafo, de la Constitución Política..."*[79]

La Sala acude a una inteligente correlación, planteada por la doctrina, entre el flujo de informaciones y el grado de democracia de un país, para ubicar ciertamente el hondo valor democrático del derecho a la autodeterminación informativa, cuyo objetivo no es detener ese flujo de informaciones, sino hacerlo transparente al ciudadano y empoderarlo para que pueda controlar aquél flujo de informaciones que lo afecte directamente en su esfera de intereses. La Sala apunta en esta dirección cuando afirma: "*...Para efectos de alcanzar una tutela de la persona realizable en el estado actual del desarrollo tecnológico, resulta indispensable considerar que los ciudadanos tienen derecho a conservar una facultad de control sobre el flujo de las informaciones personales que circulan en el entorno social. No en vano se ha venido estableciendo una relación biunívoca entre la cantidad de información que circula y la democracia, no sólo como manifestación de la entidad del derecho al acceso a las informaciones como supuesto para el desarrollo humano y social, sino también como un fundamento indispensable de la democracia, a fin de garantizar el libre desarrollo de la personalidad y la transparencia de la democracia. En la medida en que los ciudadanos puedan alcanzar un control sobre las informaciones que sobre sí mismos circulan en*

[79] Sala Constitucional, Voto No. No. 5802–99 de las 15:36 horas del 27 de julio de 1999 (Principios del Tratamiento de Datos Personales).

todos los ámbitos, en la misma medida podrá alcanzar las condiciones para evitar que el Estado o los particulares lo conviertan en una mera pieza del engranaje del poder, rebajándolo, en tal supuesto, a gozar de los ámbitos de libertad que el Estado quiera otorgarle y no aquellos que le corresponden como persona titular de una dignidad irreductible"[80].

La Sala demostró que conoce profundamente del problema e intuye que los grandes acervos de información se erigen amenazantes contra las posibilidades de autodeterminación de la persona. Junto a las ingentes posibilidades de almacenamiento, ubica nuestro Tribunal Constitucional las crecientes capacidades de procesamiento, que han hecho posibles comparaciones de datos que hace apenas una década parecían imposibles, abriendo la puerta a enormes posibilidades para controlar los ciudadanos en sus escogencias sexuales, políticas, literarias, en suma, de todos los ámbitos de desarrollo de su personalidad. Por ello, es que razona que no es posible sostener que todo lo que es posible tecnológicamente sea posible frente a los fines de tutela constitucional, o de un simple equilibrio de los intereses colectivos frente a los derechos individuales. Simplemente, no es posible entender un status civitatis en la sociedad informatizada, sino se cuenta con una facultad de control del flujo de informaciones como la que pretende delinear nuestra Sala Constitucional, a través de la puerta estrecha del habeas data. Por su importancia, transcribimos estas valiosas apreciaciones de la Sala:

"(...) La protección del derecho a la intimidad ha evolucionado con el desarrollo de los medios de información y comunicación, cuyo nivel de complejidad ha permitido el archivo de cantidades de datos cada vez más grandes sobre las personas y ha abierto la posibilidad de procesar esa información con un alto grado de precisión y en muy poco tiempo, por lo que, con este avance, sus ataques no sólo se tornan más frecuentes sino también más graves. Actualmente, el desarrollo de la informática ha hecho que los medios con que cuenta el Estado como los particulares en el almacenamiento y transmisión de información adquiera dimensiones que hasta hace poco tiempo eran insospechadas. A la capacidad de almacenamiento debe sumarse la capacidad de manejo de la información, es decir, la posibilidad de que, con el uso de tecnologías de

[80] Sala Constitucional, Voto No. No. 5802–99 de las 15:36 horas del 27 de julio de 1999 (Principios del Tratamiento de Datos Personales).

avanzada, se dé una comparación, simplificación y acomodo de datos que era imposible o muy difícil con medios manuales. Los datos reservados y clasificados en bases de datos o en cualquier otra forma de almacenamiento de información pueden ser utilizados con distintos fines, provocándose una lesión a principios básicos constitucionales no sólo por producir nuevos contextos para la información sino por permitir una imposibilidad de control de las informaciones que los ciudadanos han entregado en la confianza que sean utilizados de determinada forma. Este conflicto, que puede ser enmarcado en forma general como un conflicto entre intereses públicos y privados, no puede ser resuelto a partir de la prevalencia del interés general sobre el particular, no sólo porque conduciría a negar al individuo como una parte indispensable de la sociedad sino porque a éste debe dotársele de la posibilidad de controlar la información que sobre él se maneja"[81].

Nuestro Tribunal Constitucional tampoco perdió la oportunidad para delinear, aun más, la garantía procesal del habeas data, como instrumento de defensa de la persona frente al almacenamiento y el uso inadecuado de la información. Para ello lo unió a una serie de principios de interpretación, como lo es el principio de proporcionalidad. Queda claro de este fallo, que el habeas data no es un mecanismo para detener el flujo de informaciones. Tal y como lo hemos venido sosteniendo en esta investigación, el derecho a la autodeterminación informativa no debe ser visto como un obstáculo al progreso o al desarrollo del Estado de Bienestar, se trata realmente de un medio para garantizar que los datos personales se traten con calidad, de una manera idónea y adecuada a los fines legales que los procesamientos deben llenar, en palabras de la Sala: "*El hábeas data no puede ser considerado como un mecanismo para atacar los archivos de información en general, ni pretende la eliminación de todo tipo de registro o banco de datos, sino que debe ser aplicado en el resguardo de los fines del tratamiento de la información, de la proporcionalidad de uso de las informaciones, de la seguridad, pertenencia y veracidad de los datos recabados, para el resguardo de datos sensibles y para permitir la realización del individuo en la sociedad marcada por el signo tecnológico. Se trata de una herramienta destinada a la defensa de las personas contra toda posible lesión sobre sus derechos constitucionales*".

[81] Sala Constitucional, Voto No. No. 5802–99 de las 15:36 horas del 27 de julio de 1999 (Principios del Tratamiento de Datos Personales).

Consciente de que el habeas data tiene problemas con la faceta preventiva que caracteriza al derecho a la autodeterminación informativa, hizo una reflexión sobre este aspecto, indicando: "*El carácter preventivo del hábeas data no le es exclusivo como mecanismo de protección del derecho a la intimidad sino que la totalidad del ordenamiento jurídico debe atender a la protección de los derechos de la persona antes de que la lesión efectivamente se produzca*"[82] .

El habeas data, ya lo hemos dicho, tiene dificultades como instrumento preventivo de lesiones. Por ello es que la Sala externa su preocupación de que no todo puede quedar referido a lo que buenamente pueda hacerse desde el plano jurisdiccional. Todo el Ordenamiento Jurídico debería hacer referencia a las medidas preventivas que permitan que el tratamiento de datos personales, ab initio, responda a una serie de principios reguladores, hoy vigentes en muchas latitudes, con el fin de que haya una efectiva reflexión sobre los riesgos que todo ciudadano enfrenta cuando sus datos son tratados inmisericordemente y sin límite alguno en la sociedad de la información en la que nos hemos convertido. Por esa razón, extienden los efectos del habeas data a los bancos de datos que ya se encuentran en funcionamiento, con el fin de evitar discriminaciones odiosas por razones políticas, religiosas, de escogencia sexual, o de cualquier otro tipo, o para evitar que la persona participe en aquellos asuntos públicos de su interés. Por su valor para orientar el estudio de la figura del habeas data, transcribimos estas importantes manifestaciones de la Sala Constitucional:

> "*Esto es especialmente cierto en el caso de la tutela de un derecho que, con ese avance incesante de la tecnología, puede haber sido lesionado groseramente cuando los órganos jurisdiccionales intervienen y tales lesiones pueden ser de muy difícil reparación. A pesar de que en principio el hábeas data fue concedido en la protección del derecho a la información, el registro de datos considerados sensibles, como los relativos a las inclinaciones políticas, religiosas, al color de piel, a las inclinaciones sexuales, a la salud de la persona interesada o a las afiliaciones sindicales o políticas, si se realizan de manera nugatoria de la autodeterminación informativa podría fomentar tratos discriminatorios, por lo que este instrumento procesal debió ser ampliado como un mecanismo de control efectivo sobre la información que ya ha sido consignada en bancos de*

[82] Sala Constitucional, Voto No. No. 5802–99 de las 15:36 horas del 27 de julio de 1999 (Principios del

datos electrónicos y manuales. La existencia de datos sensibles y la posibilidad de que se manifiesten conductas discriminatorias con su manejo, entendiendo por discriminación el darle un trato a alguien no teniendo en cuenta su situación objetiva sino en función de sus rasgos como el sexo, situación familiar, color de piel, pertenencia o no a una determinada raza, etnia o religión, opinión política o gremial, ideología, origen nacional o social, posición económica, estado civil, condición física, enfermedad, elección sexual o procedimientos judiciales pendientes o finiquitados, ha marcado también un punto importante en la evolución de este instituto."[83]

Sin embargo, el Voto bajo análisis no se queda únicamente en las facultades de acceso, actualización y de confidencialidad, que pueden ser otorgadas mediante la interposición de un habeas data, sino que también puede cubrir a aquellas personas afectadas por datos que han sido desviados del fin original de su recogida, o cuando el tratamiento de datos de suyo sea prohibido, planteando incluso la opción al derecho al olvido, es decir, a los plazos dentro de los cuales un dato pierde interés a seguir siendo mantenido en el banco de datos y deba ser borrado. Es así como postuló que el derecho a la exclusión tiene las siguientes características:

"d.) Derecho a la exclusión: se refiere a la recolección de la denominada información sensible, de manera que por medio del hábeas data la persona puede solicitar la cancelación de los datos consignados y evitar así los eventuales tratos discriminatorios por parte de las personas que tengan acceso a ella. El sujeto puede solicitar la cancelación del dato registrado cuando su recolección ha sido prohibida, cuando sea impertinente para la finalidad perseguida por la base de datos o en el supuesto de que, por el transcurso de tiempo, no resulte necesario mantener el dato en el registro"[84].

Este Voto hace un valioso aporte a la discusión nacional sobre los principios

---

Tratamiento de Datos Personales).

[83] Sala Constitucional, Voto No. No. 5802–99 de las 15:36 horas del 27 de julio de 1999 (Principios del Tratamiento de Datos Personales).

[84] Sala Constitucional, Voto No. No. 5802–99 de las 15:36 horas del 27 de julio de 1999 (Principios del Tratamiento de Datos Personales).

reguladores del tratamiento de datos personales[85]. Al postular la necesidad de transparencia, está indicando no sólo que las condiciones del procesamiento tienen que ser conocidas por las personas afectadas, sino también recibir información sobre las etapas del procesamiento y de las posibilidades de intervención que le competen. Todo esto con el fin de que el ciudadano pueda ejercer un control sobre los datos que ha entregado y sobre el posible destino que éstos puedan tener. No se trata únicamente de poder "corregir" o "actualizar" datos e informaciones, como podría esperarse de una simple gestión procesal de habeas data, la Sala agrega que aun es indispensable que haya condiciones para que el tratamiento de datos pueda cumplir con altas exigencias constitucionales que implican, a su vez, el cumplimiento de otras garantías y derechos individuales. La separación de poderes informáticos, por ejemplo, que implica, entre otras cosas, que las diversas secciones o lugares de procesamiento estén separadas, resultan una consecuencia práctica de este aserto, como lo podría ser, también, en caso de que esto llegue a convertirse en una práctica consecuente: en producir una verdadera tutela sistémica (Systemdatenschutz).

En cuanto al tema de la información al afectado, mucho se ha discutido si es consecuente proveerle con una gran cantidad de indicaciones técnicas sobre cuál será el destino de sus datos, y las diversas etapas de procesamiento que serán necesarias, así como los detalles de hardware y software implícitos, temas todos que podrían ser incomprendidos por el ciudadano. Más bien la información que es necesario proveerle, para que el tratamiento de datos sea transparente, es la que es indispensable para que la persona pueda ejercer ampliamente sus derechos, es decir, conocer quien es el responsable del fichero o del banco de datos, adónde debe acudir en caso de necesitar información, así como cuál es el fin al cual quedarán sometidos los datos que entrega.

Uno de los principios más importantes es el de sujeción al fin legal para el cual se

[85] Principios que han venido siendo reconocidos en normativas internacionales como en la Directiva sobre Protección de Datos de la Unión Europea y, por ejemplo, en la Ley de Protección de Datos de Inglaterra. Dichos principios se orientan a la creación de instancias de control y vigilancia, condiciones dentro de las cuales puede considerarse un tratamiento de datos legal, reglas sobre procesamiento de datos sensitivos sobre la raza, preferencias sexuales, historioa clínica, filiación política o religiosa de una persona, provisiones de carácter procedimiental para la notificación, registro e información a los afectados, tutela específica a los periodistas y a quienes hagan valer válidamente su derecho a expresarse, así como las regulaciones sobre transferencias allende las fronteras de datos personales. Al respecto Guadamuz, Andres, Habeas Data: The Latin-America Response to Data Protection, en: http://elj.warwick.ac.uk/jilt/00-2/guadamuz.html

entregaron originalmente los datos. En el Voto bajo análisis se dijo con claridad que sin el cumplimiento de esta condición, la de definición de los usuarios autorizados, la determinación de los plazos de caducidad de los datos contenidos, no podía autorizarse el funcionamiento de un centro de acopio de datos[86].

El listado de principios incluido en esta importante sentencia se complementa con los siguientes:

- La necesidad de un organismo de control que vele porque el tratamiento automatizados de datos cumpla los principios que protegen el derecho de los ciudadanos a su autodeterminación informativa.

- Los principios de evitación de la recolección de ciertos datos (Datenvermeidung) y de ahorro en la mencionada recolección (Datensparsamkeit) son incluidos por nuestro Tribunal Constitucional, estableciendo correctamente que debe haber una limitación a la recolección de datos, de tal manera que *"… los que sean efectivamente recogidos y tratados se adecuen a solo los necesarios para el cumplimiento del fin que se haya especificado en la legislación"*[87].

- Se subraya que los "… *datos recogidos deben limitarse a la finalidad para la que fueron recogidos"*[88].

- El derecho al olvido, los datos no pueden ser mantenidos indefinidamente en un banco de datos, transcurrido ese plazo deben ser destruidos.

La obligación de confidencialidad de aquellos que laboran en centros de acopio de información también es considerada por este importante fallo, y establece claramente la correlación de este deber con el de prohibir el acceso a los datos a aquellos no autorizados. Es por ello que debe haber un verdadero código de ética interno en el Centro de Tratamiento de Datos de tal manera que se garantice "…*que los datos que se manejan sean tratados en forma confidencial de manera que se limite el acceso de*

[86] Sala Constitucional, Voto No. No. 5802–99 de las 15:36 horas del 27 de julio de 1999 (Principios del Tratamiento de Datos Personales).
[87] Sala Constitucional, Voto No. No. 5802–99 de las 15:36 horas del 27 de julio de 1999 (Principios del Tratamiento de Datos Personales).
[88] Sala Constitucional, Voto No. No. 5802–99 de las 15:36 horas del 27 de julio de 1999 (Principios del Tratamiento de Datos Personales).

terceros a la información y la tergiversación de los fines por los que fue creado el registro..."[89]

- El principio de calidad instruye que los centros de tratamiento de datos personales deben "… *asegurar la máxima veracidad y precisión de las informaciones contenidas en el banco de datos, manteniéndose completas y actualizadas…"*[90]

- El derecho a la información del afectado implica, ciertamente proveerle con detalles "…*sobre la finalidad y uso de los datos así como el derecho de acceso y rectificación de la información que sobre su persona constan en el registro..."*[91]

- El principio de proporcionalidad, en concordancia con los subprincipios de necesidad, idoneidad y prohibición de exceso en el tratamiento de datos personales, establece una serie de condiciones para el procesamiento de datos, principalmente con la razón de ser de la recogida de datos. Es por ello que, correctamente, se establece en el fallo que los datos deben tener una "justificación social", es decir, "… *los datos deben tener un propósito general y de uso específico socialmente aceptable"*[92].

- El principio de licitud exige no sólo normas claras para regular el procesamiento de datos, sino también respeto al principio de proporcionalidad. Consecuencia de ello es que los medios empleados para la recolección deben ser lícitos. El afectado no debe ser engañado. Debe prestar su consentimiento libre e informado para que dicho tratamiento de datos sea acorde con los principios constitucionales. La Sala señala este compromiso de principio de la siguiente forma: *"Principio de limitación de los medios de recolección: los mecanismos de recolección de información deben ser lícitos, es decir con el consentimiento del sujeto o con la autorización de la ley."*[93]

---

[89] Sala Constitucional, Voto No. No. 5802–99 de las 15:36 horas del 27 de julio de 1999 (Principios del Tratamiento de Datos Personales).
[90] Sala Constitucional, Voto No. No. 5802–99 de las 15:36 horas del 27 de julio de 1999 (Principios del Tratamiento de Datos Personales).
[91] Sala Constitucional, Voto No. No. 5802–99 de las 15:36 horas del 27 de julio de 1999 (Principios del Tratamiento de Datos Personales).
[92] Sala Constitucional, Voto No. No. 5802–99 de las 15:36 horas del 27 de julio de 1999 (Principios del Tratamiento de Datos Personales).

[93] Sala Constitucional, Voto No. No. 5802–99 de las 15:36 horas del 27 de julio de 1999 (Principios del Tratamiento de Datos Personales).

En cuanto a este último aspecto, el del consentimiento, con razón el Tribunal Constitucional hizo importantes consideraciones, quizá por el tipo de datos que eran objeto de cuestionamiento: los de la historia crediticia. Este tipo de datos, calificados como de interés público por la importancia de la materia en el sector bancario y financiero, son los que más recursos de amparo de tipo de habeas data han generado en los últimos años. Los recurrentes suelen ser personas que han sido afectadas por datos incorporados en ciertas protectoras de crédito, que luego venden acceso a su banco de datos a empresas bancarias y financieras. Algunas veces este tipo de consultas hacen referencia a información desactualizada o no concordante con la realidad económica del afectado, quien muchas veces debe gestionar directamente ante la protectora de crédito o ante la institución bancaria para demostrar que su historial de crédito está limpio y que es una persona digna de obtener ayuda para sus proyectos económicos.

Al respecto de estas informaciones considera la Sala que no se puede poner como expreso requisito el consentimiento de una persona que tiene deudas y no las honra para autorizar un procesamiento. Aun cuando esto tiene lógica, debe tenerse en cuenta que no todos los datos de carácter crediticio tienen una relevancia totalmente pública. Las posibilidades reales de dañar a una persona hasta reducirla a una verdadera capititis diminutio social son muy grandes cuando los datos de su historial crediticio son manejados sin respeto a los principios del tratamiento de datos esbozados en este fallo. Entre los más importantes podemos citar los principios de sujeción al fin y el principio de calidad, que obligan a las empresas protectoras de crédito a seguir un estándar mínimo de veracidad de los datos que garantice a los ciudadanos no ser objeto frecuente de injustas negativas de crédito, solo porque la base datos no es precisa ni veraz[94].

Al respecto de la relevancia pública de las informaciones crediticias ha dicho la Sala que estas informaciones son públicas, en virtud de que han sido recopiladas de registros y fuentes públicas, consistiendo el servicio de estas empresas protectoras de crédito en un simple poner a la orden estas informaciones a quien las necesite para decidir sobre el otorgamiento de un crédito. La jurisprudencia de este Alto Tribunal indica que si las fuentes son públicas, la información obtenida no daña el derecho a la intimidad. Así lo

[94] Ver Considerando X del Voto de la Sala Constitucional, No. No. 5802–99 de las 15:36 horas del 27 de julio de 1999 (Principios del Tratamiento de Datos Personales).

ha reconocido en los fallos 1999–2563 y 1999–4847. Claro está, esta apreciación proviene de la mera consideración de las fuentes de donde proviene la información. Muy distinto es si lo que hay que valorar si el tratamiento de datos ha seguido los principios sentados por la misma jurisprudencia constitucional, como el de calidad, el de sujeción al fin o el de proporcionalidad. Creemos que en constelaciones de casos donde esté planteado un problema de principios, habría, a pesar de la fuente pública donde se obtuvo la información, obligación de declarar con lugar el recurso de amparo por la afectación que se ha provocado al derecho a la autodeterminación informativa del afectado[95].

No hay problema cuando se trata de datos que están destinados a ser conservados confidencialmente, como los de las historias clínicas de la Caja Costarricense del Seguro Social. Frente a este tipo de informaciones imperan las restricciones genéricas impuestas por la misma jurisprudencia de la Sala.

Bibliografía

Cebrián, Juan Luis, La Red, Barcelona, Punto de Lectura, Santillana de Ediciones S.A., Tercera Edición, 2000. (citado como "La Red")

Chiriboga Zambrano, Galo, La acción de amparo y de hábeas data: garantías de los derechos constitucionales y su nueva realidad jurídica, en: http://www.ildis.org.ec/amparo/hab.htm

Chirino, Alfredo, La tutela de la autodeterminación informativa como un nuevo bien jurídico penalmente tutelado. El caso del Proyecto de Código Penal de Costa Rica de 1995, en: Revista Nueva Doctrina Penal, Buenos Aires, Argentina.

[95] Sobre el tema de la exactitud y precisión a la que están obligadas estas protectoras de crédito se refirió el Voto 2000–1119.

Chirino Sánchez, Alfredo, Autodeterminación Informativa y Estado de Derecho en la Sociedad Tecnológica, San José, CONAMAJ, 1997. (citado como "Autodeterminación")

Córdoba Ortega, Jorge; Fallas Vega, Elena; Ramírez Altamirano, Marina, Valerín Rodríguez, Constitución Política de la República de Costa Rica. Concordada, Anotada y con resoluciones de la Sala Constitucional, San José, Costa Rica, Asamblea Legislativa, Investigaciones Jurídicas, S.A., Centro para la Democracia, 2. Edición, 1996.

Dammann/Simitis, Bundesdatenschutzgesetz mit Landesdatenschutzgesetzen und Internationalen Vorschriften, Baden-Baden, Nomos Verklagsgesellschaft, Séptima Edición, 1995.

Däubler, Wolfgang, Klebe, Thomas, Wedde, Peter, Bundesdatenschutzgesetz. Basiskommentar, Köln, Bund Verlag, 1996. (citado como: Däubler, y otros, BDSG, Sección y No. m.)

Dronsch, Gerhard, Nochmals: Datenschutz in der Informationsgesellschaft, en: Revista Zeitschrift für Rechtspolitik, 1996, pp. 206 ss.

Gozaini, Osvaldo Alfredo, El proceso de habeas data en la nueva ley, en: http://www.abogarte.com.ar/habeasdata1.html

Guadamuz, Andres, Habeas Data: The Latin-America Response to Data Protection, en: http://elj.warwick.ac.uk/jilt/00-2/guadamuz.html

Hassemer, Winfried, Datenschutz und Datenverarbeitung Heute, Wiesbaden, 1995.

Hassemer, Winfried, Über die Absehbare Zukunft des Daztenschutzes, Revista Kritische Justiz KJ (Alemania) 1996, pp. 103 y ss.

Jacob, Joachim, Bundesbeauftragter für den Datenschutz, Dringender Handlungsbedarf für mehr Datenschutz auf dem nicht-öffentlichen Sektor, Pressemitteilung en: http://www.bfd.bund.de/aktuelles/pm19990504.html

Kloepfer, Michael, Geben moderne Technologien und die europäische Integration Anlass, Notwendigkeit, und Grenzen des Schutzes personenbezogener Informationen neu zu bestimmen?, en: Revista Neue Juristische Wochenschrift NJW, 1998, p. 21. (citado como "Technologien")

Krempl, Stefan, Grundfeiler des Datenschutzes in der vernetzten Welt, en: http://www.heise.de/bin/tp/dl-artikel.cgi?artikelnr=11108&rub_ordner=inhalt&mode (citado como: "Grundfeiler")

Losano, Mario, Das italienische Datenschutzgesetz, en: Revista Computer und Recht (Alemania), Nr. 5 de 1997.

Nogala, Detlef, Moderne Überwachungstechnologien. Zum Stand der Kunst, en: Bürgerrechte und Polizei/CILIP 60 (2/98).

Padilla, Miguel, Bancos de Datos y Acción de Habeas Data, Buenos Aires, Abeledo-Perrot, 2001.

Pérez Luño, Antonio, La tutela de la Libertad Informática, en: Agencia de Protección de Datos (Edit.), Jornadas sobre el Derecho Español de la Protección de Datos Personales, Madrid, De Arellano S.L., 1996, pp. 93 y ss.

Pérez Luño, Antonio, Los Derechos Humanos en la Sociedad Tecnológica, en: Losano/Pérez Luño/Guerrero Mateus, Libertad Informática y Leyes de Protección de Datos Personales, Madrid, Centro de Estudios Constitucionales, 1989.

Podlech, Adalbert, Das Recht auf Privatheit, en: Perels, Joachim (Edit.), Grundrechte als Fundament der Democratie, Frankfurt am Main, Suhrkamp, 1. Edición, 1979, pp. 50 y ss.

Romeo Casabona, Carlos, Tendencias Actuales sobre las Formas de Protección Jurídica ante las Nuevas Tecnologías, en: Revista del Poder Judicial, Madrid, España, No. 31, Septiembre de 1993, pp. 163-204.

Sagués, Néstor Pedro, El Habeas Data: Alcances y Problemática, en: Sánchez, Alberto, El derecho público actual. Homenaje al Prof. Dr. Pablo A. Ramella, Buenos Aires, Depalma, 1994.

Scholz, Rupert y Pitschas, Rainer, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, Berlin, Dunker und Humblot, 1984. (citado como: Selbstbestimmung)

Simitis, Spiros, Konsequenzen des Volkszählungsurteils: Ende der Übergangsfrist, en: Revista Neue Juristische Wochenschrift, 1989, p. 21. (citado como "Konsequenzen")

Simitis, Spiros, Dammann, Ulrich, Geiger, Hansjörg, Mallmann, Otto, Walz, Stephan, Kommentar zum Bundesdatenschutzgesetz, Baden-Baden, Nomos Verlagsgesellschaft, 4. Edición nuevamente revisada, julio de 1994. (citada según el autor y el número de parágrafo y número margen del texto, ej. Simitis y otros, BDSG, Parg. 9, No.m. 7).

Weichert, Thilo, Gefangen im Netz der Datenbanken, en: http://www.humanistische-union.de/hu/10publikationenordner/grundrechte_report1997/06.htm (citado como: "Gefangen")

Informes de los Comisionados de la Protección de Datos de los Länder:

Mecklenburg-Vorpommern

Fünfter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern, en: http://www.lfd.m-v.de/informat/index_in.html

Schleswig-Holstein

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 20. Tätigkeitsbericht (2001), http://www.datenschutzzentrum.de/material/tb/tb23/kap7.htm

Expedientes Legislativos:

Expediente Legislativo Número 12827 con el título „Adición de un nuevo capítulo IV, denominado „Del Recurso de Habeas Data“, al título III, de la Ley de la Jurisdicción Constitucional, Ley No. 7135, del 19 de octubre de 1989“, San José, Costa Rica, Proyecto de Ley presentado por el Prof. Dr. Constantino Urcuyo en 1996.