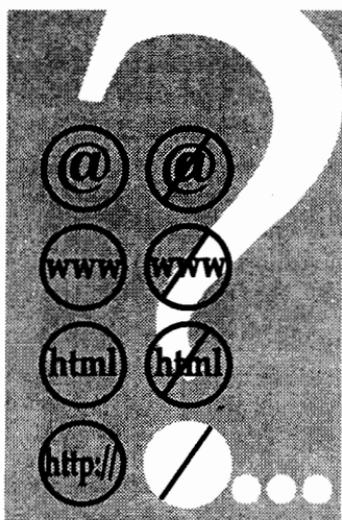


**AUTODETERMINACIÓN
INFORMATIVA
Y
ESTADO DE DERECHO
EN
LA SOCIEDAD TECNOLÓGICA**

Lic. Alfredo Chirino Sánchez



**AUTODETERMINACIÓN
INFORMATIVA
Y
ESTADO DE DERECHO
EN
LA SOCIEDAD TECNOLÓGICA.**

*Una contribución al estudio de los retos
y problemas existentes para alcanzar la
protección del ciudadano frente al
tratamiento electrónico de sus datos
personales.*

por:

Alfredo Chirino Sánchez LL.M.
(Francfort del Meno)
Profesor de Derecho Penal e Informática Jurídica
Universidad de Costa Rica

342 . 207 . 286

Ch 54 1a

Chirino Sánchez, Alfredo

Autodeterminación informativa
y Estado de Derecho en la Socie-
dad Tecnológica. -- San José,
Costa Rica : CONAMAJ, 1997.

71 p. : 21 cm.

ISBN 9968-9772-6-8

I. DERECHO CONSTITUCIONAL. II. HA-
BEAS DATA. 1. Título

CONTENIDO

PROLOGO.....	I
NOTA A LA PRIMERA EDICION.....	II
1. Rasgos particulares del actual ambiente de la información	1
2. Peligros provenientes del procesamiento de datos personales	10
3. Surgimiento del derecho a la autodeterminación informativa	14
4. El papel de las leyes de protección de datos en la evolución jurídica de la tutela de la persona frente al procesamiento de datos personales	17
5. La introducción del "habeas data" como una forma de tutela de la autodeter- minación informativa en Costa Rica y sus problemas	20
a. El "Habeas data" como forma de protección de la persona frente al tratamiento de datos personales en Costa Rica.....	24
b. El bien jurídico protegido según el Proyecto.....	26
c. El concepto de Datos Personales.....	33
e. Los requisitos para el ejercicio del Habeas Data.....	36
f. Sobre la problemática de los datos sensibles y la fase de transmisión de los datos.....	39
g. El procesamiento de datos personales realizado por la Administración Pública y los particulares.....	41
h. La no especificación de los principios derivados del derecho a la protección de datos en el articulado de la Reforma.....	42
i. Informaciones y debido proceso.....	44
j. Aspectos que aún deben de ser considerados en el Proyecto.....	49
6. Conclusiones Generales.....	53
7. Apéndice.....	59
8. Bibliografía.....	66

PRÓLOGO

La Comisión Nacional para el Mejoramiento de la Administración de Justicia tiene el honor de publicar una obra que es, no sólo necesaria, sino es urgente.

El ensayo del licenciado Alfredo Chirino "Autodeterminación Informativa y Estado de Derecho en la Sociedad Tecnológica" trata un tema contemporáneo de los más delicados e interesantes. En los tiempos presentes el manejo de la información es vital en la esfera individual, así como en la social, política y económica. De ahí que quien concentra este recurso, o quien pueda acceder a los bancos de datos electrónicos, tiene una posición de control sobre el otro de grandes magnitudes. El desarrollo de nuevas tecnologías y la integración de éstas en redes informáticas y telemáticas potencia, como nunca antes, esta posibilidad.

Cuando navegamos por Internet, por ejemplo, dejamos una estela que puede ser rastreada y de la que puede extraerse una cantidad de datos que permite elaborar un perfil sobre el navegante, con información que antes solo estaba en la mente del individuo. La información considerada irrelevante en épocas pasadas, ahora sistematizada electrónicamente, cobra importancia y arroja facetas desconocidas de los grupos sociales y sectores, generales y particulares. De estas recopilaciones se pueden crear bases de datos que podrían permitir formas de control por parte de los particulares y del Estado tampoco antes imaginadas.

Por esto es que el tema de esta obra, la protección el ámbito de la intimidad y más ampliamente, la autodeterminación informativa, son tópicos fundamentales que debemos debatir de cara a la constitución de una opinión pública libre y que cree el espacio necesario para el ejercicio pleno de los derechos fundamentales.

El autor es un jurista riguroso y un agudo investigador de los nuevos problemas que presentan las tecnologías de la comunicación a la ciencia del derecho. Es Máster en derecho de la Universidad de Francfort del Meno, República Federal de Alemania y doctorante en la misma universidad, precisamente con el tema de la tutela de la autodeterminación informativa en el proceso penal y los problemas modernos de la investigación criminal por medio de las tecnologías de información y la comunicación.

Lic. Ana Virginia Calzada M.
Vice-Presidenta CONAMAJ

Lic. Sara V. Castillo Vargas
Directora Ejecutiva- CONAMAJ

NOTA A LA PRIMERA EDICIÓN

El presente trabajo surgió con motivo de un análisis realizado por el autor de la primera versión del Proyecto de Reforma a la Ley de la Jurisdicción Constitucional presentado por el Diputado Dr. Constantino Urcuyo en 1996, con el fin de incluir el recurso de hábeas data en Costa Rica. Su original razón de ser era básicamente explicar algunos temas del derecho a la protección de datos y algunos aspectos del contexto tecnológico y social de la reforma, que consideraba importantes como parte del estudio legislativo de este importante proyecto. Es por ello que es un hijo de su tiempo, y he querido mantener su estilo expositivo a fin de que sirva como documento de discusión.

En el tiempo transcurrido desde nuestras primeras aportaciones al estudio de esta propuesta del pre-legislador costarricense, muchas cosas han sucedido. Entre ellas, y muy satisfactoria, ha sido la incorporación del texto alternativo con algunos cambios, que aparece en el apéndice de este libro, como la versión definitiva del proyecto para los debates parlamentarios. También ha sido esencial la visita a Costa Rica en setiembre de 1997, donde pudimos revisar las artes finales de este libro y dictar algunas conferencias sobre el tema de la autodeterminación informativa y el hábeas data, las cuales permitieron dar a conocer el proyecto e iniciar la discusión en el foro nacional. Fueron muy enriquecedoras las discusiones realizadas con el Prof. Dr. Rodolfo Piza, Magistrado de la Sala Constitucional; la Comisión Permanente de Asuntos Jurídicos de las Asamblea Legislativa, quien nos invitara a referirnos acerca del proyecto; y los debates con los colegas Defensores y Defensoras Públicos; y con los Procuradores y Procuradoras de la República, a quienes pude plantear algunas inquietudes científicas relacionadas con las consecuencias del hábeas data para el Proceso Penal y para la actividad del Estado.

Quiero agradecer muy especialmente a la Licda. Sara Castillo, Directora de la Comisión Nacional para el Mejoramiento de la Administración de Justicia (CONAMAJ), y a su equipo de trabajo, la gentil invitación para presentar estas reflexiones en forma de libro y por velar porque esta obra viera la luz pública en una coyuntura muy importante para la discusión legislativa del Proyecto. También quiero hacer extensivo mi agradecimiento al Señor Edgar Monge, Asesor Parlamentario y al Dr. Constantino Urcuyo, quienes me han mantenido informado de la discusión del proyecto por vía de INTERNET e hicieron posible, a pesar de la distancia, que pudiera incidir de alguna manera en el destino final de la propuesta legislativa.

Por sus muchas ideas que me han enriquecido; y por un debate inteligente sobre las tendencias del Proyecto deseo agradecer a la Licda. Gloriana López Fuscaldó.

Deseo dedicar esta obra, como siempre, a mi esposa Mariela Fernández Rodríguez, y a mis hijas, Sofía y Valeria quienes con su apoyo y sacrificio personal han hecho posibles no sólo esta obra sino también todas mis otras realizaciones personales, y muy especialmente a Fabiola, nuestra tercera hija, quien ha nacido en medio de todas estas tareas dándole un sentido especial y un impulso definitivo a todos nuestros proyectos.

El autor.

Tres Ríos, 30 de setiembre de 1997.

"...el moderno procesamiento de datos no sólo puede más sino que puede alcanzar otras cosas distintas de las que eran posible mediante el clásico sistema de percibir hechos y de anotarlos en actas. Al procesamiento automatizado de datos le falta el remedio del olvido, el cual de manera misericordiosa hace caer un velo sobre errores y fracasos haciendo posible, de esta manera, el futuro. El moderno procesamiento de datos puede delinear estructuras y pintar cuadros que por medio de la simple utilización de la vista del observador nunca hubiera sido posible poner en conjunto. Constituye, por ello, un rearme del Leviatán controlador, regulador y castigador, al cual con razón temen los seres humanos y ante el cual actúan, en la medida de lo posible, con precaución".

Winfried Hassemer, *Datenschutz und Datenverarbeitung Heute*, Wiesbaden, 1995, p. 11.

1. RASGOS PARTICULARES DEL ACTUAL AMBIENTE DE LA INFORMACIÓN

Estamos viviendo en la actualidad un verdadero movimiento en el llamado "ambiente de la información", donde los datos e informaciones han adquirido un enorme valor económico¹. El manejo de estas informaciones se ha ido haciendo a la vez sencillo así como atrayente, así como la tecnología encargada de su procesamiento se ha ido adaptando a los cambiantes y vertiginosos desarrollos de la telemática, lo que ha permitido superar fronteras temporales y geográficas, haciendo que las informaciones alcancen cualquier rincón del planeta en cuestión de segundos².

Hablamos hoy más que nunca de un mundo caracterizado por el acopio, procesamiento y transmisión de cantidades ingentes de datos. Este ambiente informativo ha hecho surgir nuevas modas, nuevos estilos de vida y formas de pensar, de comunicarnos, de observar el mundo y los acontecimientos, y la tendencia indica el rumbo hacia mayores cambios³ hasta en la forma de la organización de las ciudades, del trabajo y de las relaciones familiares, entre otros. Los desarrollos tecnológicos no se detienen. En forma vertiginosa se anuncian, diseñan, y producen equipos cada vez más pequeños y poderosos, que multiplican miles de veces el poder informático en manos de los usuarios de estos sistemas⁴.

¹ Weis, Kurt, Die Informationsgesellschaft: Zum Wandel der Menschenbilder unter neuen Technologien, en: Tinnefeld/Philipps/Weis (Edit.), Institutionen und Einzelne im Zeitalter der Informationstechnik, München; Wien, R. Oldenbourg Verlag, 1994, p. 25

² En este sentido: Lucas Murillo de la Cueva, Pablo, El Derecho a la Autodeterminación Informativa, Madrid, Tecnos, 1990, p. 106.

³ Cfr. sobre estos cambios y su incidencia en la actual configuración social: Davara Rodríguez, Miguel Angel, De las Autopistas de la Información a la Sociedad Virtual, Pamplona, Editorial Aranzadi, 1996, pp. 81 ss. Muchos de estos cambios, como por ejemplo, en la vida social, en los ritmos de trabajo, y en las reglas del orden económico, fueron pronosticados con gran claridad en el visionario trabajo de Alvin Toffler, La Tercera Ola, publicado en 1980.

⁴ Cada seis meses se duplica la velocidad de procesamiento de los computadores, según un principio establecido por la industria de la informática. Ya se ha anunciado la aparición de un procesador para computadoras personales con una velocidad de 300 Megahertz para setiembre de 1997, que supera ampliamente el estándar de 133 y 166 Megahertz que se había establecido para fines de 1996, y el de 200 Megahertz establecido con el procesador de INTEL MMX PRO apenas a inicios de 1997. Esta velocidad vuelve ridículo también el estándar de los años 80 que estaba restringido en las computadores personales a 12 megahertz. El nuevo procesador permitirá manejar y administrar recursos informáticos para la mejor utilización de imágenes y video en el computador del hogar, además de

No sólo la idea de distancia y de cercanía ha sido transformada por la llegada de este imperio de la "información", sino también la percepción de lo que se dio en llamar en la década de los años ochenta como "opinión pública". La nueva sociedad de la información⁵ hizo su entrada triunfal asegurando tener la capacidad de poner a disposición los datos relevantes para el sistema político, lo que podría llevar a una garantía de "apertura", donde todas las informaciones, no sólo aquellas conformes al sistema, circulen, abriendo el camino, según Häberle, para formular alternativas en la teoría y en la práctica, en definitiva, para producir "...la garantía de una relación de competencia entre ideas, argumentos e intereses"⁶, lo que bien podría ser la promesa de una democracia participativa verdadera⁷.

acelerar las otras funciones de esa máquina. Igualmente se ha anunciado la salida de paquetes de software que permitirán sacar provecho a todo ese poder informático ahora al alcance de una gran cantidad de personas.

⁵El término "information society" fue acuñado, según Dordick y Wang, a principios de los años 60. Este concepto es relacionado, usualmente con las tecnologías informática y de telecomunicaciones. Se espera de ella la formación de un nuevo orden social más eficiente y centrado en la producción de conocimiento, liberando al hombre de actividades repetitivas a fin de que pueda disponer de más tiempo para otras ocupaciones relacionadas con el intelecto y el espíritu. Pero hay que acotar que aún en las sociedades donde el intercambio informativo tiene un papel importante, como los Estados Unidos y Japón, no produce la información la más importante entrada de ganancias a la economía. Dordick y Wang prefieren referirse a la "sociedad de la información", como también lo hacemos nosotros, como una sociedad que toma conciencia del valor de la información para el desarrollo, y que trata de utilizarla en todos los aspectos de la vida para hacerla más eficiente y productiva. La información tiene valor en todos los rincones del mundo y para todas las personas, y tiene un papel que cumplir para mejorar las condiciones de vida. La información, como siempre, no vale por sí misma sino en la medida que pueda ser utilizada o para crear más conocimiento o para mejorar las actividades en la que sea empleada. La sociedad de la información es, en este sentido, una sociedad dirigida a la utilización de la información. Un uso que puede generar riesgos y que deben ser evitados a toda costa. Cfr. sobre los problemas de la sociedad de la información y su impronta economicista en: Dordick, Herbert y Wang, Georgette, *The Information Society. A retrospective View*, Newbury Park, London, New Delhi, Sage Publications, 1993, pp. 129 ss. Bühl señala por su parte que la primera aparición del concepto "sociedad de la información" se dio en un estudio elaborado por Daniel Bells en 1973, titulado „The Coming of Post-Industrial Society“, donde él señala una serie de características esenciales de este tipo de sociedad. El término en todo caso ha sido muy discutido. Sobre esta discusión y sus diversas manifestaciones v. Bühl, Achim, *Cybersociety. Mythos und Realität der Informationsgesellschaft*, Köln, Papy Rossa Verlags GmbH & Co. KG, 1996, pp. 28 y ss.

⁶Häberle, Peter, *Verfassung als öffentlicher Prozeß. Materialien zu einer Verfassungstheorie der offenen Gesellschaft*, Berlin, Duncker und Humblodt, 2. Edición aumentada, 1996, p. 117.

⁷Cfr. sobre esta problemática Cerqueira Leite Seelander, Airton, *Democratização pelos "Mass Media"?: O direito de ser informado e os limites fáticos à sua plena eficácia*, in: *Revista da Faculdade de Direito, Universidade de São Paulo, Brasil*, v. 83, ene-dic 1988, pp. 318 ss.

Podemos hablar del surgimiento de una "aldea global" caracterizada por infinidad de uniones neuronales que comunican equipos descentralizados de procesamiento de datos y métodos de comunicación cada vez más eficientes y veloces, los cuales hacen posible el incesante movimiento de la economía globalizada.

La radio y la televisión permitieron, como lo afirma con razón Frossini, una difusión de los mensajes de manera "omnicéntrica" (en sentido radial, que puede ser recibida en todas partes), superando la manera de comunicación únicamente entre dos puntos (como con el telégrafo y el teléfono)⁸. Por ello se constituyeron en los puntales de una nueva sociedad: la "sociedad de la información", la cual no sólo dependería de los datos propiamente dichos que serían transmitidos sino también de su relación inescindible con los medios dispuestos para su transmisión o comunicación. Estos medios han hecho posible, hoy día, que el teléfono, el telégrafo, pero también la televisión y la radio, de la mano de la telemática y de la miniaturización, se conviertan en herramientas de enorme importancia. La telefonía celular, el facsímil, la televisión y radio digitales han hecho su ingreso en la moderna "sociedad de la información", y han aumentado las posibilidades de transmisión, a escala planetaria, eliminando límites geográficos y temporales⁹. No es para nosotros una sorpresa observar "en vivo" la producción de sucesos históricos y de la naturaleza en cualquier rincón del globo terráqueo, gracias a estos medios de comunicación vía satélite, la que nos ha desligado de antiguas ataduras que impedían la percepción o la distorsionaban. Hoy tomamos parte de los sucesos, formamos nuestra opinión, nos informamos y actuamos de acuerdo a este verdadero bombardeo de datos que llega a nuestras manos.

La unión entre medios de procesamiento de información y de comunicación no se ha detenido allí. El computador se ha convertido ahora en el núcleo de muchos de estos sistemas. Hardware y software al alcance de muchas personas convierten a esta máquina de cálculo no

⁸Frossini, Vittorio, Hacia un derecho de la información, en: *Informática y Derecho*, Extremadura, España, UNED, No. 12-15; 13-14; 1996, p. 809.

⁹Frossini, op. cit., p. 810.

sólo en el centro neurálgico de acceso a la información (por vía de facsímil¹⁰, teléfono, video), sino que también es el puente para acceder a INTERNET, la cual ha abierto el debate sobre las "autopistas de la información"¹¹ ya no como el medio, sino como el mensaje mismo, parafraseando aquí a McLuhan.

a. Tras las huellas de la "aldea global"

INTERNET ha extendido sus caminos por todo el mundo y a ella se encuentran unidos millones de usuarios. Por ella transitan datos e informaciones de todos los tipos: visuales, sonoras, de texto, etc., que han llevado el conocimiento en todos los campos a todos los rincones del planeta, haciendo que el acceso y la lectura de tales magnitudes de información se haga depender de la instalación y pericia en el manejo de equipo computacional. Hoy casi que no se habla en círculos tecnológicos y de negocios de otra cosa, y no en vano se ha convertido INTERNET en tema de variadísimos debates jurídicos, cuya intensidad es directamente proporcional a la inmensa difusión de esta red y a la evidente bondad y

¹⁰ El uso cada vez más extensivo de los "modems" como aparatos para enviar facsímiles, hace que una cantidad mayor de documentos en la administración pública y privada sean generados, transmitidos y recibidos, así como revisados y editados en la forma de "documentos electrónicos". Todo ello puede realizarse sin haber impreso una vez el documento de que se trate, ello cambia, totalmente, la forma en que se piensa un documento y manifiesta el papel importantísimo de la tecnología en funciones de apoyo esenciales. Cfr. en relación con los cambios producidos por la tecnología de la información en la actividad empresarial, Cohen, Frederik, *Protection and Security on the Information Superhighway*, New York, Chichester, Brisbane, Toronto, Singapore, John Wiley & Sons, 1995, pp. 14 y ss.

¹¹ Para muchos autores, INTERNET no es la "autopista de la información" y hasta afirman que, probablemente, la mencionada "autopista" nunca llegue a existir en la forma que ha sido proclamada, entre ellos, y con bombos y platillos, por el Vicepresidente de los Estados Unidos de América Al Gore (Gore, A., *La infraestructura nacional de Datos (NII) de los Estados Unidos de América: "Agenda para la Acción"*, Traducción de Rafael Fernández Calvo, en: *Revista Novática, Asociación de Técnicos de Informática*, Barcelona, julio-agosto 1994, pp. 3 y ss.). Pero es claro que la mayoría de las informaciones que hacen alusión a la "autopista de la información" se refieren a INTERNET, una red que tuvo su origen en el año de 1969 con la así denominada ARPANET desarrollada por la Advanced Research Projects Agency, la cual unía instalaciones dedicadas a la investigación en la Costa Este y Oeste de los Estados Unidos de Norteamérica. Luego seguiría como antecesora la malograda BITNET con base estructural de IBM, también como unión de centros de Investigación. Cfr. Stegbauer, Christian, *Euphorie und Ermüchterung auf der Datenautobahn*, Frankfurt/Main, Dipa, 1996, pp. 9-10.

también a la perversidad¹² de muchos de sus servicios y a los beneficios presentes y futuros que promete a quienes están presentes en ella¹³.

El ambiente de la información del que hoy gozamos no depende como antes del libro y de la capacidad del lector para leerlos, ni tampoco de la interconexión entre dos puntos geográficos, sino ahora más que nunca de los recursos multimediales que ofrece el computador y del acceso global que éste permite. Hoy son accesibles a cualquier consumidor los discos compactos que contienen enciclopedias inmensas, grabadas en una

¹²Ha sido foco de escándalo en el mundo la apertura de servicios de INTERNET que promocionan la prostitución infantil, lo que ha generado una discusión sobre la necesidad de regular el tipo de servicios que se ofrecen en la "NET" lo que no coincide con el principio de libertad que la inspira. Recientemente en la República Federal de Alemania fueron absueltos un hombre y una mujer que ofrecían un servicio por INTERNET de localización de niños y niñas a fin de realizar con ellos prácticas sexuales y de tortura. Como un adicional ofrecían, en caso de muerte del menor, hacerse cargo del cadáver por una suma adicional. La absolución fue acordada por el Tribunal de Instancia de la ciudad de Traunstein con base en el principio del in dubio pro reo, al considerar que la oferta de los servicios antes indicados nunca fueron indicados en serio. La absolución ha causado un gran revuelo en círculos relacionados con la tutela de los niños frente a abusos y ya la fiscalía ha decidido apelar ante el Tribunal Federal.

El Tribunal de Traunstein en Baviera realizó un análisis en un terreno jurídico sumamente nuevo, cual es el de la discusión sobre si es posible realizar conductas criminales en el ciber-espacio, concentrándose la acción imputable a la propuesta de servicios en un Web-Site, sin prueba ulterior de que se hubieran realizado en efecto prácticas sado-masoquistas en menores de edad, con resultado de muerte.

¹³Del 7 al 4 de abril de 1997 tuvo lugar en la Ciudad de Bonn, en la República Federal de Alemania, la Conferencia de los G-7 sobre el tema de los mercados de trabajo globales para pequeñas y grandes empresas (EU-Nachrichten Nr. 14 del 9 de abril de 1997, p. 3, en: Revista Neue Juristische Wochenschrift, München, Frankfurt/Main, Verlag C.H. Beck, 1997, p. XLIII). En esta reunión, se llegó a determinar que mientras un 98 % de las grandes compañías cuentan con una conexión a INTERNET sólo un 4 % de las pequeñas y medianas tienen acceso a la Net. Entretanto, las compañías más grandes consideran de importancia prioritaria este acceso, así como la pronta configuración de las herramientas de software que sean necesarias para realizar negocios en el llamado "ciberespacio", que no es más que las invisibles conexiones mundiales de millones de computadores con acceso a la "red de las redes". Junto a ello señala Mario Monti, Comisario de la Comisión Europea, que serán necesario, además, asegurar la privacidad de los participantes en la comunicación, así como brindar herramientas jurídicas que protejan los derechos intelectuales de los productos que se negocien en medios virtuales, una especie de organización internacional para la protección de la propiedad intelectual ("World Intellectual Property Organisation"). Estos aspectos señalan el importante papel económico de INTERNET y la competencia que se está dando en todos los niveles por tener acceso a ella y conquistar sus secretos para afianzar un lugar en los mercados globales, los cuales en el futuro se ubicarán en INTERNET, si creemos al menos en las tendencias actuales. Las conexiones por cable de cobre se transformarán pronto en conexiones de fibra óptica que mejorarán cien veces la actual capacidad y permitirán unir la World Wide Web a una verdadera velocidad de comunicación, logrando superar la triste etapa actual de la "World Wide Waiting" como se le designa agríamente haciendo alusión a los largos tiempos de espera para recibir en el computador una página de INTERNET.

superficie de aluminio de forma digital, en donde es posible tener música, imágenes de video, sonido y texto, que le dan una particular utilidad a estos medios en la enseñanza. De la misma manera se están grabando todo tipo de datos (leyes, jurisprudencia, información didáctica sobre todos los temas e intereses) a fin de ofrecer acceso rápido y confiable a grandes acervos de informaciones que le permitan a los usuarios mejorar su capacidad de trabajo y de hacer observable el panorama abrumador de conocimientos que hoy son necesarios en todos los campos del saber¹⁴. Casi no es posible actuar en este ambiente de información sin la ayuda de las tecnologías de la información y de la comunicación, las que se encuentran en un maridaje indefectible y trascendental.

Contrariamente a los presagios esparcidos en los años setenta, el procesamiento de datos se realiza hoy de manera descentralizada¹⁵, en cada vez más poderosos aparatos, los cuales se empequeñecen conforme avanza a velocidades impresionantes la miniaturización de los procesadores y otros elementos imprescindibles de esta herramienta de cálculo. Hoy en día se pueden realizar complejos procesos en máquinas que poseen miles de veces el poder computacional que tenían los computadores que echaron andar la informatización de la administración pública a principios de los años setenta. El tamaño de estos computadores es incomparable con el de aquellos monstruos pertenecientes ya a la prehistoria de la informática.

Esta miniaturización ha permitido que el procesamiento de datos se divorcie de la administración centralizada y que ésta no dependa más de la generación de ingentes bancos de datos, sólo debe asegurarse el acceso a los datos almacenados por los particulares, quienes realizan, hoy más que nunca, un inmenso y detallado acopio de todos los datos imaginables sobre las personas¹⁶.

¹⁴Weis hace referencia al "hijo de la sociedad de la información" denominado "el idiota de la era de la información", el cual superará el viejo principio de que el "idiota especializado" sabe demasiado sobre muy poco. El "idiota de la era de la información" sabrá muy poco de una gran cantidad de conocimiento disponible. Cfr. Weis, Informationsgesellschaft, p. 33.

¹⁵Simitis, Spiros, Virtuelle Präsenz und Spurenlosigkeit - Ein neues Datenschutzkonzept, Krit V 1996, pp. 99 ss.

¹⁶Las policías han empezado a valorar la necesidad de estar presentes en INTERNET y realizar allí

Los consumidores de servicios de INTERNET son viajeros que dejan una huella indeleble de su paso, como lo ha afirmado recientemente el Comisionado Federal de la Protección de Datos de la República Federal de Alemania Joachim Jacob. Infinidad de datos personales pueden ser recolectados de los diversos lugares donde el usuario ha hecho entrada para auscultar la oferta inmensa que está a disposición de aquellos que entran a los llamados "Web Sites"¹⁷. No sólo los importantes datos relacionados con la actividad financiera o los mismos números de tarjeta de crédito¹⁸ están a disposición de quien, con la pericia necesaria, quiera

investigaciones sobre delitos como el de la pedofilia. La policía de Baviera, en Alemania, ha anunciado la presencia de su propia página en la Net ("<http://polizei.bayern.de>"), donde se incluye informaciones sobre sospechosos tales como fotografías, retratos hablados, datos de contextura física y sobre el peligro que pueda representar para los ciudadanos, y se solicita colaboración de la población. Esta actitud de la policía bávara sigue el ejemplo de la FBI que recién tuvo éxito en la búsqueda de un sospechoso, quien durante años había logrado escapar a la policía federal estadounidense y gracias a las pistas obtenidas de un ciudadano que reportó la presencia del sospechoso en Guatemala vía INTERNET, fue detenido y puesto a las órdenes de las autoridades. Esta tendencia despierta preguntas sobre la legalidad de estos medios de investigación, y la mayor parte de preguntas brotan de un razonable temor al manejo de datos personales, producto de las colaboraciones de los ciudadanos, en INTERNET, un tema abierto para la discusión.

¹⁷ Se trata de los "sitios" o lugares que pueden ser visitados en el ciberespacio de "INTERNET". El concepto de "WebSite" se desarrolla a partir diferentes direcciones que trabajan bajo el concepto "cliente/servidor". Un servidor, que es un computador que ha sido colocado para dar apoyo al funcionamiento a la determinada página o "site" de INTERNET contiene "hiperdokumentos" que pueden ser llamados desde cualquier parte de la red con un "browser" o "cliente", el más popular de ellos es actualmente el "Netscape". Los "hipertextos" provienen de un concepto de Ted Nelson, quien en 1965 los concibió como textos que no son lineales sino que contienen relaciones a otros documentos, estas relaciones son llamadas hoy en día "hyperlinks" o "hiperuniones" que producen al ser marcadas por el usuario una conexión inmediata con otras páginas de la World Wide Web (WWW).

¹⁸ Bühl reporta que una de las compañías que ofrecen servicios de acceso a INTERNET en los Estados Unidos fue víctima de la acción de un "Hacker", quien tuvo acceso a los archivos grabados en el computador central de la firma y hurtó los datos correspondientes a más de 40,000 números de tarjetas de crédito, los cuales hubieran podido ser utilizados en muchas actividades delictivas como la estafa de compañías que ofrecen servicios en-línea, como también para revender estos datos, los cuales tienen un gran valor en el mundo comercial. Estos y otros ejemplos demuestran que INTERNET aún está lejos de tener un estándar de seguridad confiable, y que el trabajo en el campo de codificación de las informaciones en esta red debe seguir teniendo la mayor prioridad. Cfr. Bühl, *Cybersociety*, op. cit., p. 238. El tema de la seguridad de los datos, y del propio procesamiento de datos se ha ido convirtiendo, mientras tanto en un campo con sentido propio, no más en una actividad secundaria en la relación de "medio para el fin" del derecho de la persona a ser protegida frente al tratamiento de datos personales, situación provocada, principalmente por la cercanía terminológica que tiene en diversas lenguas el derecho a la libertad informática y a la seguridad de los datos ("data protection"; "data security"; "Datenschutz"; "Datensicherung"; "protección de datos")

apoderarse de ellos, sino también información, podríamos llamar inferencial, sobre aspiraciones, uso del tiempo libre, filiaciones políticas, y hasta sobre la escogencia sexual, todos ellos datos que pueden ser referidos a una persona o grupo de personas por medios tecnológicos. Tenemos, en este sentido, una "presencia virtual"¹⁹ absolutamente transparente para el control²⁰.

Nuestra personalidad se ha hecho transparente para aquellos que desean conocer nuestros gustos²¹ y apetencias, para los que eventualmente nos podrían emplear o asegurar, también para aquellos que deciden en

El derecho a que el procesamiento de datos se dé de una manera confidencial, con fidelidad, integridad y seguridad ha adquirido últimamente una importancia enorme y por ello ha adquirido una independencia del derecho a la autodeterminación informativa, y constituye tanto como éste una forma de desarrollar garantías informacionales en la actualidad. Cfr. al respecto, Fiedler, Herbert, *Informationelle Garantien für das Zeitalter der Infomationstechnik*, en: Tinnefeld/Philipps/Weis, *Institutionen*, pp. 150-151.

¹⁹ Simitis, *Virtuelle Präsenz*, op. cit., p. 104.

²⁰ El tema de la protección de los datos personales en INTERNET ha generado intensas discusiones, en las que han intervenido autoridades de los Estados Unidos y de la Unión Europea (UE), según lo informó el periódico costarricense "La Nación", del día 14 de julio de 1997. La UE exige a los Estados Unidos, según este informe periodístico, que garantice la protección de los datos personales que son enviados a través de la red durante las transacciones comerciales, de lo contrario prohibiría el envío de datos privados a los Estados Unidos. Este último país está convencido de que el control y tutela de los datos ha de ser una preocupación del sector privado dedicado a estas actividades, las cuales generaron mil millones de dólares en 1996, y con un crecimiento e importancia siempre en aumento. El Estado, según las autoridades estadounidenses, no debería involucrarse en la regulación de esta materia que ocasione trabas al libre comercio de datos e informaciones, solo en un caso ineludible serían necesarias leyes simples que promocionen y favorezcan el desarrollo de los intercambios comerciales. Así, ellos optan por dejar a la iniciativa privada el desarrollo de políticas de protección y de los sistemas tecnológicos necesarios para garantizar esa protección. El que dicha política tenga algún éxito es algo aún por verse y mientras tanto la UE se sujeta a su propia tendencia hacia la tutela jurídica de las personas frente al tratamiento de sus datos personales y la Directiva que en esa materia entrará en vigencia para el año de 1998.

²¹ Mediante el análisis del número de consultas "interactivas" a un catálogo de productos en INTERNET es posible recuperar datos sobre los artículos solicitados y, por ejemplo, cuáles páginas del catálogo han sido más consultadas por los clientes, lo que permite formar perfiles de personalidad de las personas que usan estos servicios, datos que luego pueden ser usados para estudios de mercados. Así como se realizan estas "inferencias" con el uso de catálogos de productos, pueden hacerse perfiles de las personas a partir de los libros que compran, de los periódicos que leen en la INTERNET, como también de sus comentarios y opiniones en los foros de discusión que existen sobre casi todos los temas imaginables en el llamado "ciberespacio". Todos estos aspectos apuntan a los peligros que ofrece a la privacidad la INTERNET, que no son del todo imposibles de vencer pero que requieren de una conciencia por parte de los usuarios y de mayores y mejores medios para el cifrado de informaciones, aspecto que tiene un grave componente político, relacionado con la voluntad de los Estados a no permitir un sistema de cifrado que no pueda ser "leído", por ejemplo, por la policía o los organismos de seguridad, ya que se piensa que sería un medio de facilitar actividades criminales o

gran medida sobre la obtención de créditos y posibilidades de financiamiento. Somos importantes también como electores, por lo que nuestra intención de voto y nuestras inclinaciones políticas han adquirido también, como las otras informaciones, un enorme valor económico²². Estos perfiles de las diversas facetas de la personalidad social e individual de los ciudadanos han cobrado un valor esencial y su manejo en banco de datos encuentra usos en todos los campos, también en el de la administración de justicia.

El intercambio de informaciones, la comparación de datos, la conformación de perfiles de personalidad, son actividades no sólo tecnológicamente posibles, sino también necesarias para perfilar la sociedad de mercado en la que estamos viviendo. Nuestras informaciones, en todos los campos, son necesarias para la toma de decisiones. Interesan a la administración pública como también a los particulares, y tanto unos como otros están apertrechados tecnológicamente para realizar una ingente acumulación de datos en forma descentralizada, que pueden ser consultados, comparados y transmitidos en fracciones de segundo a cualquier lugar del mundo²³. Tal poder no es más un tema de novelas de ciencia-ficción como la premonitoria alegoría de George Orwell en su obra "1984". El estado total que puede realizar una vigilancia cuidadosa de todos nuestros movimientos, escogencias, inclinaciones, virtudes,

subversivas sin que el Estado pueda hacer nada por impedirlo al no contar con los medios para descifrar los mensajes que son enviados por correo electrónico, o cualquier otro medio de los usuales de INTERNET. Sobre esta problemática v. Bühl, op. cit., pp. 238-239.

²² En época pre-electoral empiezan a realizarse los famosos "censos" donde los partidos políticos sondean la filiación política de los ciudadanos, sus colaboraciones en anteriores campañas, el tipo de cooperación prestada y la disponibilidad para participar en la siguiente campaña, todo esto con el nombre, número de cédula y dirección del votante, lo que permite no sólo realizar un sondeo de la intención de voto en el lugar del "censo", sino también una descripción amplia y exacta del perfil del votante. Dichos datos son utilizados tanto para fines estadísticos (anonimizados, probablemente) y para fines de elaborar padrones de votantes para las mesas de votación durante el día de las elecciones. Este tipo de censos, despierta, por supuesto, una serie de interrogantes acerca de la legalidad y conveniencia de conservar tantos datos personales en los sistemas de información de los partidos políticos.

²³ Algunas compañías que ofrecen acceso a INTERNET facilitan a sus clientes el envío de mensajes por medio del correo electrónico, sin embargo, re-conducen los mensajes enviados entre dos puntos de un país y los envían a otro, digamos Estados Unidos, donde no existen las mismas regulaciones sobre protección de la privacidad y de la autodeterminación informativa, y allí los mensajes pueden ser analizados y filtrados de cualquier manera, lo que genera, como lo propone Bühl, reflexiones sobre el concepto de "soberanía estatal" en el ciberespacio, y sobre el papel importantísimo de una tutela internacional, con idénticos estándares, de la autodeterminación informativa de los ciudadanos. Cfr. Bühl, op. cit., p. 239.

pecados y esperanzas es hoy una realidad, gracias a la herramienta de la tecnología de la información y de la comunicación²⁴.

2. PELIGROS PROVENIENTES DEL PROCESAMIENTO DE DATOS PERSONALES

Como tantas otras herramientas de la historia, esta tecnología puede producir también una gran dimensión de beneficios, pero también una enorme cantidad de riesgos y peligros para el ciudadano, los cuales muchas veces pasan desapercibidos producto del carácter sutil e incruento y hasta atractivo de sus promesas. Estamos dispuestos a canjear nuestra libertad a cambio de seguridad, aún cuando esta promesa sólo tenga efectos simbólicos. El canje no es obligatorio, pero lo aceptamos como necesario, ya que se presenta a nosotros como inevitable, es más, como el único medio, en una época en que imperan los medios y donde, como bien lo decía Albert Einstein, se da una gran confusión de fines. En el camino para obtener más "seguridad", comprometemos nuestra libertad. Abriendo la puerta a la tecnología, sin ninguna reflexión de sus problemas, la aceptamos como la panacea para los problemas de la humanidad. Si bien la tecnología puede producir muchos beneficios, también entrega en las manos de los organismos de control los hilos para la definición de nuestro presente y de nuestro futuro.

²⁴ En una encuesta realizada por Eurobarómetro en 1995 (Cfr. Davara, op. cit., p. 26), donde se entrevistaron 500 personas provenientes de cada uno de los países de la Comunidad Europea se logró percibir que para los ciudadanos europeos no resultaba familiar la "sociedad de la información". De la encuesta puede deducirse que uno de cada dos de los europeos no sabe siquiera definir en qué consistía, pero que sí todos ellos estaban recelosos de lo que la tecnología podría traer para sus vidas, un 57 % de los europeos opina que estos avances pueden traer graves riesgos para su intimidad. Los porcentajes más altos de preocupación se lograron percibir en Irlanda, Francia y Alemania, pero en todos los países de la Comunidad Europea fue claro que los entrevistados manifestaron reservas y temores. Esto no resulta extraño tomando en cuenta los grandes debates suscitados en los últimos años en los países europeos dirigidos a agilizar la aprobación de leyes que permitan la escucha de apartamentos con aparatos cada vez más sofisticados, así como la observación de largo plazo de personas, así como el acceso a datos personales por parte de la policía y de los organismos de inteligencia del Estado, con la posibilidad de intercambiar información entre ambos a fin de realizar pesquisas de delitos de amplio espectro, donde no sólo los sospechosos de cometer los hechos delictivos resultan incluidos en las investigaciones sino también personas inocentes, que por razón de los datos que alguna vez entregaron entran en la red de la investigación. Sobre esta problemática puede ser consultada la obra de Leuthardt, Beat, *Leben on Line. Von der Chipkarte bis zum Europol-Netz: Der Mensch unter ständigem Verdacht*, Reinbeck bei Hamburg, Rowohlt Taschenbuch Verlag, 1996, pp. 100 ss.

El moderno procesamiento de datos resulta ser no sólo sutil y carente de violencia²⁵, sino que también es seductor y apetecido. Sus peligros no suelen percibirse ya que los mismos se ocultan ante los beneficios que se obtienen. Se vende el "valiente nuevo mundo" con la promesa de mayor seguridad, menos burocracia, más eficiencia y velocidad en las actividades de la agresiva sociedad de mercado. En este "mercadeo del futuro" se oculta el hecho del procesamiento de datos móvil y descentralizado, de la comercialización de la información; de la interconexión de los bancos de datos, y del papel del Estado de observador participante, el cual comprende mejor que antes que ahora sólo tiene que asegurarse un acceso a los bancos de datos particulares para alcanzar la mayor parte de sus objetivos de control. El ciudadano se encuentra aquí confuso y hasta desinformado. Algo está pasando y él no lo comprende, ya que lo que sucede se oculta en el vestido del avance y del progreso, y contra esta promesa, una actitud reservada y meditativa tiene las peores cartas.

Los peligros que han surgido a partir del desarrollo de este particular "ambiente informativo" que vivimos, pueden verse claramente si reflexionamos un poco acerca de los "efectos colaterales" de este papel protagonista de los datos personales en la sociedad de mercado. Como lo afirma el Prof. Winfried Hassemer, anterior Comisionado para la Protección de Datos del Land Hesse y hoy Juez del Tribunal Constitucional Federal alemán, las posibilidades de inspección a la vida interior de la persona son cada vez más grandes²⁶. Ya los motivos, las costumbres, los impulsos e instintos, las inclinaciones, las dependencias y los vicios, no serán más tema del ámbito privado, el Estado y los particulares pueden observar y registrar todo esto y de una manera rápida y fácil. Los nuevos medios de control y vigilancia, no sólo "...permiten ver más profundamente sino también amplían el ámbito de visión"²⁷. La técnica que hace posible esto se hace cada vez menos transparente mientras hace posible que la personalidad de los ciudadanos y su fuero interno se hagan cristalinos para el control²⁸.

²⁵ Este carácter incruento de la vigilancia tecnológica modifica cualitativamente la naturaleza de esa vigilancia, como lo dice José Antonio Martín, Magistrado del Tribunal Supremo Español citando a Gary Marx, haciéndola rutinaria, además de contar con la posibilidad de ampliarla y profundizarla, no siendo necesario utilizarla para evitar golpes de estado o revoluciones, se puede usar todos los días y no depende de si cae o no en malas manos, lo que subraya su evidente tendencia totalitaria. Cfr. Martín Pallín, José Antonio, Constitucionalidad del Número de Identificación único, en: Agencia de Protección de Datos, Jornadas sobre el Derecho Español de la Protección de Datos Personales, Madrid, 1996, pp. 62.

²⁶ Hassemer, Winfried, *Datenschutz und Datenverarbeitung Heute*, Wiesbaden, 1995, p. 20, en el mismo sentido, Martín Pallín, op. cit., pp. 59 y ss.

²⁷ Hassemer, *Datenschutz*, op. cit., p. 20.

²⁸ Hassemer, *Datenschutz*, p.20.

Las condiciones del ambiente de información en nuestro país, que con la tecnología instalada, y las aplicaciones que ya hoy día tienen un amplio mercado y un gran número de usuarios, hacen posible que la personalidad de los ciudadanos se haga transparente, especialmente para el Estado, quien tiene un obvio interés en estos datos, no sólo porque facilitan diversas gestiones consignadas en sus fines constitucionales y de organización, sino porque permiten un más eficiente control social de los ciudadanos. Control que hoy podría significar la realización de una sociedad "panóptica" donde los ciudadanos no encontrarían espacios donde desarrollar su individualidad, y donde poco a poco el ejercicio de sus derechos quedaría supeditado a algunas pequeñas zonas donde el Estado eventualmente no tendría interés en introducirse²⁹.

Esta situación llevaría poco a poco, como lo analizan ampliamente algunos autores europeos, como el Prof. Dr. Spiros Simitis, ex-Comisionado de la Protección de Datos del Land Hesse y Profesor de la Universidad de Francfort del Meno³⁰, a que muchas garantías y derechos individuales se conviertan, en esencia, en letra muerta, ya que muchos ciudadanos tendrían temor al ejercicio de los mismos, ante la posibilidad de que el Estado los estigmatice y controle cuando decidan ejercerlos³¹.

Como lo afirma con claridad Simitis, con cada paso que se da en dirección a un procesamiento técnicamente mejorado de los datos personales, se produce, al mismo tiempo, un cambio en las condiciones de comunicación dentro de la sociedad, y la pregunta que surge aquí de

²⁹ En Costa Rica ya se han presentado casos graves relacionados con el manejo de datos personales. El mismo Proyecto de Ley para introducir el "Habeas Data" en Costa Rica, relata los prejuicios que se le causaron a un ciudadano al ser incluido injustamente, sin su consentimiento y sin saberlo, en un listado de morosos de un banco, luego de muchas gestiones, y más de tres años de no obtener ningún crédito producto de su inclusión en ese listado, logró, por intermedio del Defensor del Pueblo, que se le excluyera de esa lista. Casos como ese han de ser muy frecuentes y probablemente son sólo la punta del iceberg de una problemática muy compleja que causa daños a muchos ciudadanos. Cfr. la referencia a este caso en la Exposición de Motivos del Proyecto de Ley presentado por el Diputado Dr. Constantino Urcuyo, bajo el Expediente 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". De seguido haremos referencia a él solamente como "el Proyecto".

³⁰ Cfr. Simitis en: Simitis/Dammann/Geiger/Mallmann/Walz, Kommentar zum Bundesdatenschutzgesetz, Baden-Baden, Nomos Verlags-gesellschaft, 4. Edición totalmente revisada, 1992, Parágrafo Primero, passim.

³¹ Cfr. Simitis, Spiros, Von der Amtshilfe zur Informationshilfe. Informationsaustausch und Datenschutzanforderungen in der öffentlichen Verwaltung, en: NJW 1986, pp. 2795 ss.

manera insoslayable, es en qué medida estaría preparado el ciudadano ante esta situación para ser consciente de su papel dentro de la sociedad, sobre el desarrollo político de una opinión, para construir su propia perspectiva y para defender lo que piensa. Si el ciudadano no tiene posibilidad de controlar quién tiene acceso a sus datos, con qué objetivos y bajo qué presupuestos, pronto tendrá que desistir del ejercicio de sus derechos fundamentales, ya que muchas libertades públicas (como la libertad de asociación y de reunión, así como las libertades de expresión y de autodeterminación) se convertirían en meras formas sin contenido, ya que aumentarían al mismo tiempo las posibilidades para la manipulación a fin de impedir o al menos amedrentar a quienes deseen ejercer tales libertades, no con prohibiciones directas, sino con la aplicación de consecuencias indirectas al mero ejercicio de un derecho. Si el ciudadano tiene acceso a sus datos, podría controlar y dirigir el sentido social de los mismos, a fin de evitar consecuencias nefastas no a su esfera íntima de manera directa, sino a su posibilidad de participación social.

La sociedad asustada con los datos sobre criminalidad y violencia que le son todos los días transmitidos por los medios de comunicación colectiva exige poco a poco, como remedio esperanzador, que el Estado se convierta, de una vez por todas, en un "Estado de Seguridad o Vigilancia"³², que produzca ese ansiado bien aún cuando se pierda libertad en el proceso. Confiado de esta nueva labor, no logramos otra cosa más sino que el hambriento Estado ahora se lance en pos de todos estos datos personales para realizar sus tareas de control y vigilancia. La reflexión sobre los derechos fundamentales en el Estado Democrático de Derecho resulta abandonada ante la "sublime visión" de una tarea estatal que encuentra refugio en el "ansia particular" de seguridad, con la trágica consecuencia de encontrarnos nuevamente ante la paradoja de nuestras esperanzas perdidas.

El derecho a la protección de la persona frente al procesamiento de sus datos personales surge así como una necesidad en el Estado de Derecho, como una necesidad de reflexión sobre los derechos y libertades públicas en juego, como también de las posibilidades de la persona humana en una sociedad tecnológica.

³² Cfr. Bölsche, Jochen (Hrsg.), *Der Weg in der Überwachungsstaat*, Reinbeck bei Hamburg, Rowohlt Taschenbuch Verlag, 1979, *passim*.

3. SURGIMIENTO DEL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA

Este ambiente global de información que hemos descrito someramente, ha puesto en entredicho el concepto tradicional de "intimidad", para dar paso a nuevos matices conceptuales, a nuevas perspectivas de comunicación entre las personas y los países, generando con ello nuevos retos para el derecho a la protección de datos, el cual se debate hoy en día entre sus ligámenes a los viejos sistemas de control, y a la necesidad de utilizar nuevas herramientas tecnológicas para garantizar el derecho fundamental de los ciudadanos a decidir quién, cuando y dónde, y bajo cuáles circunstancias, toma contacto con sus datos.

Es así como es posible encontrar hoy día trabajos como el de Schmitt Glaeser, quien sostiene que una protección de la esfera de la vida privada, es esencialmente una "protección de la información"³³. Este tipo de propuestas ofrecen un amplio elenco de posibilidades para articular la tutela de la intimidad bajo el entramado básico de la facultad del ciudadano de controlar el uso de las informaciones que lo puedan afectar. En esta línea se ubicaría por ejemplo la propuesta de Shattuck para la definición de la privacy en cuatro esferas esenciales, en donde la número cuatro, se referiría directamente a la facultad de control de las informaciones (information control).

Como lo señala Pérez Luño, la definición de esta tendencia de concebir la privacy como una posibilidad del control de informaciones se encuentra ya en el libro de Alan Westin "Privacy and Freedom", quien a finales de la década de los años 60 planteó el derecho del ciudadano a controlar las informaciones sobre sí mismo "a right to control information about one self". Esta tendencia también fue seguida por Lusky (Invasion of Privacy) y por Fried (Privacy, 1968), ambos subrayando claramente la necesidad que los ciudadanos controlen la información que les concierne, ya no como un mero derecho de defensa frente a las intromisiones de otros, sino ahora, y frente a los riesgos tecnológicos, como un derecho activo de control sobre el flujo de informaciones que circulan sobre todos nosotros.

³³ Schmitt Glaeser, Walter, Schutz der Privatssphäre, en: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts, Heidelberg, Bd. VI, 1989, pp. 41 ss.

La justificación para otorgar este "status positivus"³⁴ del ciudadano se vincula directamente con la tutela de la dignidad de la persona humana, con la necesidad de proteger el libre desarrollo de la personalidad, y con el afianzamiento de la libertad en la sociedad democrática, ya que el control de las informaciones "...aparece como una condición para una convivencia política democrática"³⁵.

No se trata de limitar el tratamiento electrónico de los datos que es, en esencia, y esto como una verificación de los posibles desarrollos futuros, una condición para el progreso de los Estados, sino más bien de luchar porque dicho tratamiento se realice de una manera democrática, afianzando los derechos y garantías del ciudadano, y promocionando la participación social de todos los seres humanos. Salta a la vista que un acceso a las informaciones públicas permitirá no sólo una mayor transparencia en el funcionamiento de las instituciones, sino también una mayor posibilidad de que los ciudadanos tengan acceso a condiciones mejores para su desarrollo individual y para el ejercicio de sus derechos políticos. Pero también hay que ser conscientes de que eso no justifica que por alcanzar la transparencia de la sociedad, los ciudadanos pierdan la posibilidad de preservar su personalidad del acceso extralimitado y

³⁴ La teoría iuspublicista de los "status" iniciada por Jellinek se busca completar hoy día con la propuesta de introducir un "status positivus socialis", que abarcaría los intereses económicos, culturales y sociales. El Prof. Erhardt Denninger de Francfort del Meno postula asimismo la existencia de un "status activus processualis", el cual tiene como fundamento la facultad de la persona de participar activamente en los procesos que le afectan, así como en las organizaciones encargadas de la tutela de sus derechos. Cfr. a este respecto, Pérez Luño, Antonio, La tutela de la Libertad Informática, en: Agencia de Protección de Datos, Jornadas sobre el Derecho Español de la Protección de Datos Personales, Madrid, 1996, pp. 94-95.

³⁵ Así, 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, p. 330. También la Prof. Ilse Staff de la Universidad de Francfort del Meno lo ha mencionado recientemente: la lucha por un derecho a la tutela de la persona frente a la protección de los datos tiene también como elemento nuclear la conciencia, al menos en el ambiente constitucional alemán, de que ha de protegerse la soberanía popular (Volkssouveranität) la cual depende, en gran medida, de los procesos de formación de la opinión de los ciudadanos. Sin un acceso libre a las informaciones, y una tutela de la persona frente al procesamiento de sus datos personales por parte de aquellos interesados en ellos (principalmente, las agencias del control estatal), podría ponerse en peligro la capacidad de intervención de los ciudadanos en los asuntos públicos y dañarse la validez formal del principio democrático de la Constitución. Cfr. Staff, Ilse, Öffentlichkeit als Verfassungsprinzip, ZRP (Alemania), p. 385.

objetivizante del Estado o de los particulares. Este dilema enfrenta 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, sino que habrá de considerarse igualmente el interés del ser humano no sólo a gozar de mayor información en todos los ámbitos del conocimiento y de la cultura ("freedom of information"), como también la necesidad de tutelar a la persona frente al uso desmedido de sus datos personales.

El nuevo papel de la intimidad, así planteado, rompe los viejos compartimentos estancos en que se desarrollaba la artificial escisión entre lo público y lo privado, entre lo personal y lo colectivo, entre lo íntimo y lo general, para abrir la puerta a la discusión sobre los espacios sociales donde se produce la interacción entre los ciudadanos para el alcance de objetivos comunes, haciendo ejercicio de nuevos matices de la libertad, potenciados por nuevas formas de comunicación .

Esta nueva dimensión de la intimidad se manifiesta prontamente en el desarrollo jurídico de la década de los setenta y los ochenta, bajo la estructura jurídica del derecho a la autodeterminación informativa, con un profundo arraigo en principios tales como la dignidad humana, la libertad individual, la autodeterminación y la democracia, que antes de ser utilizados como puntos de sustentación vacíos y sin contenido, adquieren una nueva perspectiva en el Estado de Derecho.

Es así como resultan, en un principio, como tareas primordiales de este derecho del ciudadano en los momentos primigenios del surgimiento de lo que hoy conocemos como "sociedad informatizada", la conservación de un ideal de ser humano que se iba convirtiendo cada vez más en una irrealidad ante los desarrollos portentosos de la técnica: el deseo de alcanzar su autodeterminación, de lograr una incidencia efectiva en su medio social, sin temor a que su participación social se redujera ante el poder ilimitado puesto en manos de los controladores al contar éstos con sus informaciones más sensibles, y pudiendo utilizarlas en las formas y dimensiones que deseara. Por otra parte, y en extrema relación con este primer objetivo, también se trataba de la tutela de un "valor material" de este ser humano, el cual se iba relativizando cada vez más no

sólo por la "movilidad" de su papel a lo interno de la sociedad, como también por la objetivación a la que tiende toda forma tecnocrática de organización. Como lo afirma oportunamente el Comisionado para la Protección de los Datos Personales de Baja Sajona Gerhard Dronsch, a propósito de su disputa con Nitsch sobre el papel de la protección de datos en la actualidad, y como crítica al acercamiento "cuasi-populista" al tema que hoy nos ocupa, "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"³⁶.

4. EL PAPEL DE LAS LEYES DE PROTECCIÓN DE DATOS EN LA EVOLUCIÓN JURÍDICA DE LA TUTELA DE LA PERSONA FRENTE AL PROCESAMIENTO DE DATOS PERSONALES

La necesidad de superar estos problemas interpretativos en relación con la "intimidad" en su nueva faceta social, y de brindar herramientas prácticas al ciudadano para ejercer facultades de control sobre sus informaciones, condujo lentamente a la incorporación en los ordenamientos jurídicos de diversas leyes de tutela que pretenden ser una forma de responder legislativamente a la evidente calidad de "agresión" que ostentaban las políticas de manejo de los datos en el ámbito público. La Ley de Protección de Datos del Estado de Hesse en Alemania fue la primera ley emitida en el mundo para garantizar al ciudadano este derecho.

En algunos países incluso el constituyente ha reconocido la necesidad de que el derecho a la autodeterminación informativa pase a formar parte del elenco de derechos fundamentales incluido en la Carta Magna.

En América Latina se han decidido por la constitucionalización

³⁶ Dronsch, Gerhard, Nochmals: Datenschutz in der Informationsgesellschaft, ZRP, 1996, pp. 206 ss.

de este derecho Colombia y Brasil³⁷, también Paraguay en la Constitución de 1992 (art. 136) y Ecuador en su reciente Constitución del 18 de junio de 1996³⁸; y en Argentina la Constitución de las Provincias de Jujuy, La Rioja, San Juan; Córdoba; San Luis; Río Negro, Tierra del Fuego y Buenos Aires³⁹ 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". Existen proyectos de legislación en Argentina, Colombia, Costa Rica⁴⁰, Chile, y Paraguay, y algunas disposiciones en el sentido de reconocer al ciudadano facultades de control sobre sus datos en Méjico⁴¹.

³⁷ El tema del habeas data en Brasil parece iniciarse con motivo de la preocupación del Prof. José Alonso da Silva por conceder un medio para que los ciudadanos tuvieran acceso a las informaciones que sobre ellos estuvieran registradas por entidades públicas y privadas. Para ello conformó una Comisión Provisoria de Estudios Constitucionales, presidida por el Dr. Alonso Arinos de Mello Franco, la cual empezaría a trabajar para encontrar un medio expedito que, al igual que el habeas corpus, permitiera la ciudadano acceso a estas informaciones. Después vendrían otros proyectos, como el "Muda Brasil" y el "Proyecto de Constitución de la Comisión de Sistematización", los cuales irían también en el mismo sentido, poniendo especial atención al acceso a informaciones en manos de entidades policiales y militares. Sobre la evolución de estos proyectos cfr. Nusdeo, Marcos y Folgosi, Rosolea, "Habeas Data", en: RDP-87, Brasil, pp. 90 ss.

³⁸ 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".

³⁹ La Exposición de Motivos del Proyecto contiene una detallada transcripción de los textos constitucionales de Argentina y de las Provincias citadas, Cfr. pp. 22 y ss.

⁴⁰ Proyecto para la inclusión del habeas data en la Ley de la Jurisdicción Constitucional, Expediente legislativo Número 12827, ya citado.

⁴¹ Estos ejemplos demuestran la imprecisión del concepto de Gartska de que desde finales de los años setenta "ninguna reforma constitucional ha llegado a discutir la aceptación del derecho a la protección de datos dentro del catálogo de derechos fundamentales". En América Latina, y esto precisamente en un proceso iniciado en los años ochenta, y con frutos ya en los años 90, ha discutido el valor de este derecho desde la perspectiva constitucional. Cfr. Garstka, Hansjürgen, Informationelle Selbstbestimmung- ein Menschenrecht?, en: Heymann, Thomas (Edir.), Informationsmarkt und Informationenschutz in Europa: rechtliche Fragen, europäische Harmonisierung/ im Auftrag der Deutschen Gesellschaft für Recht und Informatik e. V., Köln, Verlag Dr. Otto Schmidt KG, 1995, p. 123.

Portugal fue el primer país europeo que constitucionalizó en el artículo 35 de su Ley Fundamental (1976) el derecho de los ciudadanos a controlar las informaciones que sobre ellos circulan, sin embargo, no sería sino hasta 1991 que finalmente se reguló por ley los aspectos concretos de esta declaración. El segundo país europeo en reconocer constitucionalmente la necesidad de tutelar al ciudadano frente a los riesgos de la informática fue España, país que tardó también catorce años en poner en práctica una ley que diera los mecanismos necesarios para alcanzar la mencionada tutela .

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 .

Actualmente cuentan con leyes de tutela también Alemania, Bélgica, Dinamarca, Francia, Irlanda, Luxemburgo, Países Bajos, el Reino Unido, Austria, Finlandia, Islandia, Grecia⁴², Noruega y Suecia. También Canadá y Japón . Italia acaba de aprobar a inicios de mayo de 1997 su Ley de Protección de Datos⁴³ .

Estas leyes demostraron ser esenciales como complemento de las garantías generales del Estado de Derecho , no sólo como limitativas de esas ansias exorbitadas de información del Estado, sino también como un método práctico y razonable para que el ciudadano pudiera acceder a sus propios datos, almacenados en diversas bases o bancos de datos, y ejercer un control sobre ellos , no en vano se ha dicho que en esta época lo que se construía con aquella tecnología tan sofisticada era ni más ni menos lo que George Orwel, en su obra "1984", había anticipado: un Estado omnipresente, con acceso a todos los ámbitos de la vida social y con la posibilidad de convertir a los miembros de la colectividad en "ciudadanos de cristal" , los cuales ya no estarían en posibilidad de guardar ningún secreto frente a aquél enorme "Leviatán" deshumanizante.

⁴² Grecia puso en vigencia su ley de protección de la persona frente al tratamiento de datos personales el 19 de marzo de 1997.

⁴³ Ley Nr. 675 del 31 de diciembre de 1996: Tutela delle persone e di altri soggetti rispetto al trattamento de dati personalli, publicada en el Supplemento ordinario alla "Gazzetta Ufficiale", Nr. 5 del 9 de enero de 1997, que entró en vigencia el 8 de mayo de 1997. La ley ha sido recientemente reseñada por Losano, Mario, Das italienische Datenschutzgesetz, en: Revista Computer und Recht (Alemania), Nr. 5 de 1997, p. 308 (Nota al pie 2).

5. LA INTRODUCCIÓN DEL "HABEAS DATA" COMO UNA FORMA DE TUTELA DE LA AUTODETERMINACIÓN INFORMATIVA EN COSTA RICA Y SUS PROBLEMAS

a. ¿Habeas Data o autodeterminación informativa?

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"⁴⁴ este concepto 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.

En la más pura versión del concepto de "habeas data" es posible encontrar vínculos con conceptos tales como el de "libertad informática", el cual Frossini define como "...el derecho de conocimiento y de autodecisión sobre los datos personales propios..."⁴⁵. Frossini también va

⁴⁴ Se trata de "traer los datos", como el "habeas corpus" pretende "traer el cuerpo" de la persona afectada por una detención ilegítima. En el sentido de Sagués se trata de "...contener ciertos excesos del llamado poder informático". 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 Artur Marques da Silva Filho, *Comentários a Constituição Federal*, Saraiva, Brasil, 1991, p. 81. De hecho fue la Constitución Federal de Brasil, el primer texto constitucional en introducir el concepto de "habeas data" como una garantía frente a los riesgos de la persecución política luego de la apertura a la democracia, riesgos que amenazaban a políticos de quienes se tenían muchas informaciones personales en manos de agencias de seguridad del Estado y que podían ser utilizadas en cualquier momento en su contra, de ahí el carácter peculiar de la regulación brasileña, impregnada muy especialmente de una reacción frente a este peligro.

⁴⁵ Frossini, op. cit., p. 812. Pérez Luño encuentra una relación entre "habeas data" y "libertad informática" y se refiere a un verdadero "status de habeas data", es decir, a una garantía para las personas de acceso y control de las informaciones procesadas en bancos de datos. Agrega este autor que dada la importancia de la "proceduralización" para la tutela de derechos fundamentales, también el derecho a la autodeterminación informativa ha sido dotado de una tutela procesal, tal y como está presente, por ejemplo, en la "Ley Orgánica Reguladora del Tratamiento Automatizado de los Datos de Carácter Personal" (L.O.R.T.A.D.) de España. Dándose entonces una vinculación entre la declaración del derecho fundamental al acceso y control de las informaciones y la proceduralización de su tutela. Cfr. Pérez Luño, *La Tutela de la Libertad Informática*, op. cit., pp. 93-95.

más allá al decir que el concepto de "habeas data" es una "metáfora más atrevida" de lo que significa la "libertad informática", quizá porque la pretensión que sirve de base al concepto de "habeas data" pueda ser en sí misma imposible o nociva, ya que no se trata de exigir los datos como si se ejerciera sobre ellos un derecho a la propiedad, sino que lo que realmente se debe de intentar proteger es el derecho del ciudadano a saber quién, cuándo, con qué fines y en qué circunstancias toma contacto con sus datos personales. Así, el derecho a la autodeterminación informativa no le concede al ciudadano un definitivo y absoluto poder sobre sus datos⁴⁶, 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 al ciudadano. 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.

En tal sentido, mientras sea entendido el "habeas data" como la realización de estas expectativas, entonces el "habeas data" se convierte en una versión, en una formulación abierta, de lo que hemos llamado "autodeterminación informativa", en un típico derecho o libertad de la tercera generación⁴⁷, siguiendo la clasificación del Profesor de Sevilla Pérez Luño, surgidos a partir del fenómeno de la "contaminación de las

⁴⁶ Scholz, Rupett y Pitschas, Rainet, *Informationelle Selbstbestimmung und staatliche Informationsverantwortung*, Berlin, Dunker und Humblot, 1984, p. 27.

⁴⁷ 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 ejemplo, a la LORTAD española. Cfr. Pérez Luño, *La Tutela de la Libertad Informática*, op. cit., pp. 97-98.

libertades" producto de determinados usos de las nuevas tecnologías⁴⁸. Se trata, en definitiva, de un derecho que se interesa ahora no sólo del factor de calidad de los datos, sino también de su funcionalidad o uso, lo que implica un mayor interés legislativo por los aspectos técnicos en que se desarrolla el procesamiento de datos personales, aspecto ineludible si se desea crear un régimen de protección adecuado⁴⁹.

Si se observan los ejemplos que se extraen del derecho comparado latinoamericano (incluyendo aquí a Brasil) es posible decir que el "habeas data" se ha convertido, sin embargo, en una mera garantía procedimental⁵⁰ al derecho del ciudadano al acceso y conocimiento de sus datos personales en registros públicos y privados. Es decir, que en el ámbito latinoamericano, lejos de luchar en dirección a la conquista de un derecho constitucional a la tutela de la persona frente a los peligros del tratamiento electrónico de datos personales, se ha pretendido abrir, con mayor o menor éxito, vías procesales de tutela, a veces confiadas a la jurisdicción constitucional, y en otros casos a la jurisdicción administrativa, para que el ciudadano, dado el caso que conozca del procesamiento y sus perjuicios, acuda a esa vía y exija acceso y eventual solicite la corrección o eliminación de los datos existentes sobre él en manos de la administración pública o de los particulares.

Esta tendencia latinoamericana, si bien loable en el sentido de que comienza el camino hacia el reconocimiento de un derecho del ciudadano a obtener información y a gozar de derechos de rectificación o de eliminación de informaciones incorrectas o lesivas que se encuentren grabadas o archivadas en registros públicos o privados, fracasa al conceder una garantía procedimental, que en la mayoría de los casos

⁴⁸ Cfr. Pérez Luño, *La Tutela de la Libertad Informática*, op. cit., p. 97.

⁴⁹ Esta unificación entre herramientas técnicas y protección de datos es promocionada, por ejemplo, por Hassemer, Winfried, *Über die Absehbare Zukunft des Datenschutzes*, KJ (Alemania) 1996, pp. 103 y ss.

⁵⁰ 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".

funcionará siempre después que sucedió la transmisión de los datos, a velocidades infinitesimales, y el daño para la personalidad ya ha sido verificado. Es decir, entre otras cosas, esta forma de tutela no potencia la prevención y los mecanismos de control antes de la producción del eventual peligro para la autodeterminación informativa. Apuesta fuertemente a que la acción va a ser realizada por el particular, sobre todo en los casos en que se trate de la recopilación de datos sensibles (como los de convicción política o religiosa, orientación sexual, datos genéticos, etc.), pero esta actividad del particular no se va a realizar si correlativamente no se garantiza el derecho del ciudadano a obtener información sobre el procesamiento o mediante la exigencia de tomar el consentimiento razonado del ciudadano frente a la posibilidad de un tratamiento electrónico de sus datos.

Un ejercicio del habeas data sin un correlativo derecho de información sobre las formas en que se realizará el procesamiento, los 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.

Otras experiencias del derecho comparado nos obligan también a ser precavidos acerca de los límites del "habeas data", por ejemplo, en el caso brasileño el constituyente restringió evidentemente la acción de esta garantía procedimental únicamente a los "bancos de datos gubernamentales o de carácter público", aún cuando algunos alegan que puede ser ejercido también frente a particulares⁵¹.

También las preguntas básicas procedentes del desarrollo legislativo y constitucional del "derecho a la autodeterminación informativa" se mantienen sin respuesta para el "habeas data". Entre estos aspectos destaca la pregunta de la forma en que se realizará el equilibrio entre los derechos en juego. Si se protege al ciudadano frente al tratamiento de datos personales, también hay que reconocer la necesidad

⁵¹ Cfr. Lippmann, Ernesto, *O Habeas Data visto pela doutrina e interpretado pelos Tribunais*, en: *Revista dos Tribunais*, Brasil, enero de 1996, v. 723, p. 117.

de brindar libertad al desarrollo tecnológico e investigativo, a los fines de la persecución de los delitos, entre otros, que forman parte del núcleo álgido de los problemas centrales del derecho a la protección de la persona frente al tratamiento de sus datos personales⁵². El otro problema, como lo menciona Sagués, se refiere a la forma de la tutela procedimental⁵³, respuesta que ya tiene forma jurídica en varios países.

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

El Diputado Dr. Constantino Urcuyo ha tenido la iniciativa, en un proyecto redactado en el año de 1996, de introducir una reforma a la

⁵² Ya en Costa Rica se han presentado casos a la Sala Constitucional de la Corte Suprema de Justicia (v. V-476-91 de las catorce horas y diez minutos del primero de marzo de mil novecientos noventa y uno en recurso de amparo presentado por A.E.M.L. contra el Organismo de Investigación Judicial) en donde ha sido necesario establecer un equilibrio entre la "funcionalidad" del registro de delincuentes y el interés de un ciudadano de que una "ficha" por una contravención no siguiera teniendo validez en su contra y de esa manera no ser más objeto de persecución policiaca. En este fallo decidió el Tribunal Constitucional costarricense no conceder el derecho a la eliminación de la "ficha" existente toda vez, según el fallo, que el ciudadano había sido objeto de una detención en 1989 y a un posterior proceso donde se le condenó por una contravención, siendo así, el Organismo de Investigación Judicial, en acatamiento de sus facultades legales, podía conservar la "ficha" con los datos personales del ciudadano. En un recurso de amparo anterior, éste sí con éxito, se alegó que un ciudadano fue objeto de una detención aparentemente sin causa justificada por parte de la policía judicial, detención que condujo a que se le confeccionara una ficha con sus datos personales. La Sala analizó en este caso que no existía una autorización legal para mantener esa ficha en poder de las autoridades del Archivo Criminal, toda vez que el ciudadano había sido detenido por error y luego puesto en libertad, de tal manera que conservar su ficha sería una violación a los principios de libertad e inocencia con rango constitucional y se ordenó pagar los daños y perjuicios ocasionados al ciudadano y a eliminar la ficha a él referida en manos del Archivo Criminal. Como puede observarse, la argumentación de la Sala Constitucional se quedó exclusivamente en el análisis de la prerrogativa a conservar los datos personales y no directamente sobre el derecho a la autodeterminación informativa del ciudadano, ni siquiera en el caso de un fichaje por contravención. Sería interesante observar si esta argumentación se mantendrá para casos en donde se alegue, legítimamente, un manejo de datos injustificado en manos de las autoridades de la persecución penal por vía del habeas data, en donde el equilibrio difícilmente podrá plantearse entre la prerrogativa a tener el Archivo Criminal y el derecho del ciudadano a no ser inquietado en su libertad por un antecedente criminal ya no más válido, sino más bien entre el derecho del ciudadano a que sus datos no estén registrados afectando su posibilidad de participación social activa, y el derecho del Estado a la "funcionalidad" de un registro criminal. La argumentación en este sentido será de enorme interés para el desarrollo futuro del derecho a la protección de datos en Costa Rica.

⁵³ Sagués, op. cit., p. 179.

vigente Ley de la Jurisdicción Constitucional No. 7135 del 19 de octubre de 1989, a fin de que se adicione 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.

El Proyecto parte de la premisa de que la estructura del recurso de amparo, que en Costa Rica tiene una gran amplitud, serviría para brindar una tutela de la libertad informática "ágil e inmediata".

En la "Exposición de Motivos" del Proyecto se considera, asimismo, que el "habeas data" es un "remedio procesal" que protege dos fases de la "libertad informática", por una parte, los datos personales en sí mismos ("habeas datas propio") y, por otra parte, el "habeas datas impropio", el cual tutela el derecho de los ciudadanos al acceso a la información, frente a la cual se tiene un "interés legítimo"⁵⁴.

Se considera en este Proyecto que 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 pretende lograr una tutela de los datos personales de los ciudadanos considerando, con razón como ya se ha visto, que el crecimiento del procesamiento de datos en manos del Estado y de los particulares ha sido tan extraordinario en los últimos años, que la puerta al abuso está abierta de par en par. Se valoran de esta manera como problemáticas y riesgosas las actividades de tratamiento de datos personales que aunque se realizan con un fin legítimo, luego resulta este fin quebrantado, o cuando los datos se utilizan con otros objetivos, o cuando

⁵⁴ Exposición de Motivos, Expediente No. 12827, p. 30.

el dato no es fidedigno o cuando se producen lesiones a la intimidad debido a escasas o inexistentes medidas de seguridad en el centro de cómputo.

Finalmente se argumenta en la "Exposición de Motivos" del Proyecto que una carencia en el sistema constitucional costarricense en relación con los peligros de la informática sería muy peligrosa, y es por ello que resulta indispensable, según los razonamientos expresados regular "la información de carácter informático". Así se opta por ampliar la competencia del Tribunal Constitucional costarricense para el análisis de estas lesiones a derechos constitucionales, y conceder al ciudadano un acceso a esa jurisdicción de manera ágil, rápida y sumaria, "acorde con los derechos en peligro".

b. El bien jurídico protegido según el Proyecto

El "habeas data" costarricense funcionaría, entonces, tutelando un amplio marco de bienes jurídicos, que van desde la "autodeterminación informativa"⁵⁵, la "intimidad" hasta la "libertad informática". Esta apreciación del ámbito de tutela deja ver que el Proyecto tiene claro que los riesgos no sólo están presentes y guardan una íntima relación con la complejidad propia de la sociedad de la información, como porque la persona en sí misma, tanto en su perspectiva "privada" como "social", se encuentra a merced de un tratamiento de datos ilimitado. Es así como el mismo Proyecto adiciona consideraciones sobre los peligros de "estigmatización del individuo" y sobre la incidencia que ésta puede tener el desarrollo del "aspecto social" del ciudadano en una democracia.

No obstante, la impresión que da el proyecto, luego de leer su articulado, es la de que constituye, principalmente, una tutela procedimental a la intimidad del ciudadano, y solo eventualmente a su derecho de ser informado. Esto se debe al énfasis puesto en la redacción del proyecto a tutelar el así llamado "habeas datas propio".

⁵⁵ Exposición de Motivos, Expediente No. 12827, p. 7.

Resulta indudable la importancia de conceder una tutela al derecho del ciudadano a tener conocimiento de quién, cómo, con qué objetivos y en qué circunstancias tiene contacto con sus datos personales, sobre todo si se toma en cuenta, como lo hace también la Exposición de Motivos del Proyecto⁵⁶, las condiciones del ambiente de información en nuestro país, que con la tecnología instalada, y las aplicaciones que ya hoy día tienen un amplio mercado y un gran número de usuarios, hacen posible que la personalidad de los ciudadanos se haga transparente no sólo a los particulares (que realizan también un procesamiento de datos personales) sino también al Estado, quien tiene un obvio interés en estos datos, no sólo porque facilitan diversas gestiones consignadas en sus fines constitucionales y de organización, sino porque permiten un más eficiente control social de los ciudadanos. Control que hoy podría significar la realización de una sociedad "panóptica" donde los ciudadanos no encontrarían espacios donde desarrollar su individualidad, y donde poco a poco el ejercicio de sus derechos quedaría supeditado a algunas pequeñas zonas donde el Estado eventualmente no tendría interés en introducirse .

Esta situación llevaría poco a poco, como lo analizan ampliamente algunos autores europeos, como el Prof. Dr. Spiros Simitis, ex-Comisionado de la Protección de Datos del Land Hesse y Profesor de la Universidad de Francfort del Meno, a que muchas garantías y derechos individuales se conviertan, en esencia, en letra muerta, ya que muchos ciudadanos tendrían temor al ejercicio de los mismos, ante la posibilidad de que el Estado los estigmatice y controle. Así muchas libertades públicas, como el derecho a sindicalización, a participar activamente en la vida política del país, o incluso el derecho al trabajo, a la libre elección de la pareja sexual, y el derecho a no ser discriminado por condiciones personales, se verían seriamente lesionados, acarreado esto que los ciudadanos ya no pudieran autodeterminarse, que no puedan realizar un plan de vida libremente escogido, eliminándose de esa manera uno de los requisitos más esenciales para la vida democrática de un país.

Este peligro se materializa cuando el Estado o los particulares

⁵⁶ Cfr. también las observaciones de la Licda. Gloriana López Fuscaldó a la primera versión del Proyecto de Reforma en: Expediente No. 12827.

tienen la capacidad de construir perfiles de personalidad de los ciudadanos, los cuales pueden ser obtenidos mediante la unificación y comparación de gran cantidad de datos, de la más diversa especie, a velocidades vertiginosas gracias al uso extensivo de herramientas de la tecnología de la información y de la comunicación.

Los datos, no importa su carácter, su nimiedad, o su escasa relevancia, tienen la capacidad de coadyuvar a la realización de estos perfiles de la personalidad de los ciudadanos, ya que los mismos no son atendidos según su singular naturaleza, sino que son comparados, reunificados y definidos en razón de una persona particular, lo que hace posible saber más acerca de los gustos, aficiones, tendencias, prácticas, estudios, costumbres, deseos, aspiraciones, taras, enfermedades, problemas y demás singularidades de una persona. Por esa razón es que ya no se puede hablar más de datos sin importancia. Para el procesamiento de datos todos los datos tienen una especial relevancia, todos los datos son útiles, y si se pueden obtener "a beneficio de inventario" mucho mejor, así se puede disponer de otra gran cantidad de datos que después pueden ser utilizados con los más diversos fines, con frecuencia totalmente distintos al fin original que respaldó su recogida.

Por lo dicho es que el bien jurídico tutelado en la reforma parece tener un problema en su definición. Si se parte que el "habeas data" tutela un conglomerado de derechos (intimidad, autodeterminación informativa y el ejercicio de todos los derechos y libertades), no queda claro como será posible esa tutela, sino únicamente a partir de una tutela patrimonializante de la intimidad⁵⁷, ya que el derecho a la "autodeterminación informativa" no existe como tal ni en la Constitución Política⁵⁸, ni tampoco existe jurisprudencia constitucional que lo defina.

⁵⁷ 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, (de pronta aparición).

⁵⁸ El artículo 24 Constitucional relacionado con la protección de la intimidad garantiza únicamente el derecho a la intimidad, a la libertad y al secreto de las comunicaciones, pero nada dice sobre el derecho del ciudadano de ser protegido frente a los riesgos provenientes del uso de la informática y las comunicaciones, aunque tal tutela podría provenir de una interpretación sistemática del artículo 24, con el artículo 1 de la Constitución, así como con el artículo 28, 30, 33 y 41, que crean un marco democrático, donde la persona es entendida como un proyecto que puede ser realizado según la voluntad, siempre y cuando no se afecten derechos de terceros, o el orden público o la moral. La protección del ser humano frente a discriminaciones y a su libertad permitiría agregar el detalle de "participación política y social" que requiere la intimidad para no ser "patrimonialmente" protegida, sino, antes bien, como herramienta de garantía para darle al ciudadano la posibilidad de ejercer otros derechos constitucionales sin temor a ser vigilado o impedido tecnológicamente de ello.

Al introducir el artículo 71 del Proyecto⁵⁹ a la autodeterminación informativa y a la intimidad como bienes jurídicos a proteger, sin ninguna definición, entonces el trabajo de interpretación sistemática de este artículo con la Constitución Política, bien podría hacer nacer una definición amplia y adecuada del bien jurídico a proteger, como también podría producir una reducida tutela de tipo patrimonial de la intimidad. como ya se expuesto en el medio nacional , toda vez que al afirmar que se protege el derecho al acceso a los datos, de alguna manera se crea una tutela patrimonializante, es decir, que crea una especie de dominio sobre los datos personales, cuando en esencia lo que debe tenerse en cuenta es la tutela del derecho del ciudadano a saber cuáles datos suyos están siendo tratados, con qué fines, por cuáles personas, bajo qué circunstancias y con el fin de definir cuáles son los peligros que para su persona los mencionados tratamientos pueden tener. Este derecho se conoce en la discusión jurídica alemana como el derecho a la autodeterminación informativa (*informationelle Selbstbestimmung*) y tiene precisamente su punto de partida en la intimidad, pero significa más que ésta, es la tutela de áreas de libertad, de las áreas en las que un sujeto puede autodeterminarse, en la gestación y desarrollo de su plan de vida. Aquí entran en funcionamiento, también tutelas procedimentales a este derecho, con el fin de que el ejercicio de otras garantías y derechos pueda ser resguardada. Es por ello que el Tribunal Constitucional Alemán, en su famosa Sentencia sobre la Ley de Censos de 1983, le dio un rango constitucional a la tutela del derecho a la autodeterminación informativa.

Si bien podría considerarse que esta objeción al proyecto tiene un carácter meramente conceptual, es necesario hacer notar que cómo no existe una determinación constitucional específica, la Sala IV tendría que atenerse al texto del artículo 24 de la Constitución y al artículo 13,

⁵⁹ Artículo 71: Habeas Data Propio. A través del recurso de hábeas data, toda persona física o jurídica, podrá conocer lo que conste de la misma o sobre sus bienes , en registro, archivos, listados o bancos de datos, sean manuales, mecánicos, electrónicos o informatizados, públicos o privados, así como la finalidad a que se destine esta información, y a requerir su rectificación, actualización, inclusión, confidencialidad o cancelación inmediata. Ningún dato será proporcionado a tercero, salvo que tenga un interés legítimo. La manipulación de la información y de los datos no podrá vulnerar la intimidad, la autodeterminación informativa y el pleno ejercicio de todos los derechos y libertades, salvo que sea para fines estadísticos..."

inciso primero, del Pacto de San José, para la interpretación no sólo de las acciones lesivas, como también para interpretar las diversas etapas del procesamiento de datos. Ambas disposiciones, a pesar de su generalidad, no alcanzan a cubrir los fines de tutela, por lo que parece hacerse necesario una definición mucho más amplia del bien jurídico a tutelar, para evitar problemas de interpretación, que en algunos casos, podrían contribuir a una limitación peligrosa del "habeas data".

La Sala Constitucional ha venido realizando, entre tanto, una interpretación del artículo 24 que se concreta en el concepto de intimidad como un "...derecho del individuo a tener un sector personal una esfera privada de su vida, inaccesible al público salvo expresa voluntad del interesado".⁶⁰ Refiere entonces 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, en primera instancia, 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 1949⁶¹, 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 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..."⁶² Y esto es así, toda vez que la mención a los procedimientos clandestinos de acceso a la intimidad no sólo abre el

⁶⁰ 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.

⁶¹ 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.

⁶² Sala Constitucional, V.3308-94 citado según: Córdoba y otros, Constitución Política, op. cit., p. 101.

frente de batalla frente al 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"⁶³.

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, 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 tutela de sus posibilidades de participación democrática⁶⁴.

⁶³ Ibid.

⁶⁴ 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 Demokratie*, Frankfurt am Main, Suhrkamp, 1. Edición, 1979, p. 52.

Si la interpretación proveniente de la Sala Constitucional se mantiene coherente sobre las líneas de esta reciente jurisprudencia es posible esperar, tarde o temprano, algún fallo de principio que sienta las bases del derecho del ciudadano a ser protegido frente a los tratamientos de sus datos personales, pero esto se producirá sí y solo sí la Sala Cuarta decide entender esta relación entre la intimidad y la democracia, es decir, como una garantía 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 reconocido⁶⁵.

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 privée" 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 circunstancias toma contacto con sus datos personales.

⁶⁵ Sala Constitucional V.678-91, citado según Córdoba y otros, en: *Constitución Política*, op. cit., p. 110.

c. El concepto de Datos Personales

En el Proyecto no se define directamente que ha de entenderse por "datos personales". El artículo 71 se limita a hacer alusión a "...lo que conste de la persona o sobre sus bienes, en registro, archivos, listados o bancos de datos, sean manuales, mecánicos, electrónicos o informatizados, públicos o privados". Esta definición plantea el problema que no se toma en cuenta lo referido a los datos anonimizados o anonimables que son utilizados en la estadísticas, y que mediante modernos sistemas de cálculo pueden ser redirigidos a las personas o grupos sociales que los han entregado, por lo que merecen una consideración especial, no sólo en cuanto a las reglas para producir esa "anonimización"; como también en lo referente a las reglas dentro de las cuales ha de moverse el trabajo en la estadística, la mayor parte de ellas vinculadas a principios como el de la libertad de investigación y de información.

Al no decir que ha de entenderse por "datos personales del recurrente" se abre la puerta a una consideración amplia de los mismos, lo que resulta conforme a las modernas tendencias en el derecho a la protección de los datos personales, en donde el carácter de los datos carece de interés ya que en el estado actual del procesamiento de datos todos los datos son importantes, toda vez que éstos pueden compararse, transmitirse y reelaborarse en fracciones de segundo con el fin de crear perfiles y cuadros completos de los ciudadanos. Los "datos personales" no están constituidos únicamente por datos alfanuméricos, sino que pueden también estar constituidos por imágenes y sonido⁶⁶. Modernos desarrollos en la tecnología de reproducción, grabación y almacenamiento de datos hace posible, hoy día, que sean tan fácilmente accesibles los datos alfanuméricos, como también informaciones fotográficas y sonoras, que pueden ser digitalizadas y accesadas vía telemática, como hoy se ofrece de manera amplia en diversos servicios de INTERNET.

d. El interés legítimo y el "habeas data impropio"

⁶⁶ Cfr. García Beato, María José, Principios y derechos en la Ley Orgánica 5/1992, de 29 de octubre, y en la Directiva 95/46 CE, en: Agencia de Protección de Datos, Jornadas sobre el Derecho Español de la Protección de Datos Personales, Madrid, 1996, pp. 36-37.

El "habeas data impropio"⁶⁷ es una institución que merece análisis aparte. Mediante esta posibilidad se puede solicitar información propia o ajena contenida en registros, listados, archivos o bancos de datos. Interesa el supuesto mediante el cual terceros pueden pedir datos personales que no les pertenecen siempre que demuestren un interés legítimo.

La base de este "habeas data impropio" no está en el sentido de la tutela de derechos personales, sino mucho más en el derecho de información, sin embargo, el pre-legislador no ha previsto, aparentemente, por ejemplo, los casos de difícil equilibrio constitucional cuando, en ejercicio del derecho de informar a otros, la prensa exija el acceso a datos e informaciones de personas que se encuentre bajo investigación periodística⁶⁸. En estos casos el interés legítimo lo harán brotar los solicitantes del derecho a informar a la ciudadanía sobre asuntos de interés público. Estas hipótesis son de difícil equilibrio, sobre todo en los supuestos de conflicto con la actividad periodística⁶⁹. En el derecho comparado se ha introducido además del requisito del interés legítimo, el requisito de que exista razones de proporcionalidad⁷⁰ para otorgar este acceso a la información.

En la Constitución de Portugal, en su artículo 35, párrafo segundo, se prohíbe expresamente el acceso a archivos o registros informáticos para

⁶⁷ Esta posibilidad está contenida en el artículo 72 del Proyecto que establece: Por medio del recurso de hábeas data se garantizará el derecho a solicitar información contenida en estos registros, listados, archivos o bancos de datos, aunque la información no verse sobre su persona o sus bienes, siempre y cuando el sujeto demuestre que tiene un interés legítimo para acceder a esta información. Este recurso procederá, asimismo, para información declarada como secreto de Estado, siendo el magistrado instructor quien deberá determinar si efectivamente esta información merece el calificativo."

⁶⁸ Al respecto, por ejemplo, Damm, Renate, "Medienprivileg" im Spannungsfeld von Informationsfreiheit und Datenschutz, en: Tinnefeld/Philipps/Weis (Edit.), Institutionen, pp. 131 y ss.

⁶⁹ Confrontar sobre esta problemática, Wegel, Wolfgang, *Presse und Rundfunk im Datenschutzrecht*, Frankfurt am Main, Peter Lang, 1995, pp. 77 ss.

⁷⁰ Sobre el principio de proporcionalidad y sus consecuencias constitucionales puede confrontarse Chirino, Alfredo, A propósito del Principio de Oportunidad y del Criterio de Insignificancia del Hecho, en: González Álvarez, Daniel, *Reflexiones sobre el Nuevo Proceso Penal*, San José, Costa Rica, Imprenta y Litografía Mundo Gráfico, 1996, pp. 130 ss.

conocimiento de datos personales relativos a terceros⁷¹. El constituyente portugués tuvo en mente, quizá, estos casos fronterizos, altamente conflictivos, y salvo la posibilidad de algún caso excepcional, el cual, como siempre debe ser revisado específicamente a fin de determinar su procedencia. El pre-legislador costarricense es mucho más ambicioso en la redacción del habeas data impropio, y deja abierto un flanco muy delicado de manejar y custodiar.

Un tema que además no ha sido considerado, y que es de radical importancia en el tema del "habeas data impropio", en caso de que se insista sobre él, es el que se refiere al tema del derecho de información del afectado. Para las hipótesis en que se entregan datos de otra persona a un tercero que está interesado legítimamente en ellos, se debería de condicionar a que el afectado reciba información sobre quién tiene interés en sus datos, por cual motivo y bajo cuáles circunstancias toma contacto con sus datos, así como sobre el hecho de si sus datos serán sometidos a un nuevo procesamiento de datos en manos de los terceros que reciben los datos personales del afectado⁷².

Una hipótesis que para nada ha sido incluida en el Proyecto y que debería de ser objeto de una legislación aparte, o de un artículo en el Proyecto cuando menos, es el de los supuestos en que el Estado, justificado en fines públicos, como el de la investigación de los delitos, persiga información personal de sospechosos y personas inocentes, a fin de realizar pesquisas electrónicas mediante comparación de grandes cantidades de datos o mediante la reunificación de datos que han sido entregados a distintas organizaciones públicas y privadas con otros fines distintos a los

⁷¹ "2. Es prohibido el acceso a los registros informáticos o ficheros para conocimiento de datos personales relativos a terceros, y la respectiva interconexión, salvo en los casos excepcionales y con la reserva de lo dispuesto en el artículo 18 (restricciones constitucionales necesarias para la salvaguardia de los derechos o garantías de otros)". Artículo 35, párrafo 2, de la Constitución Portuguesa, según la revisión de 1989.

⁷²

Idéntica problemática introduce la reciente Directiva 94/46 de la Comunidad Económica Europea en relación con la LORTAD española, al respecto cfr. García Beato, op. cit., pp. 46 y ss.

de la investigación criminal⁷³. En éste como en otros supuestos debe de exigirse la existencia de una normativa específica, que además de ser clara establezca como límite el principio de proporcionalidad a fin de que en cada caso en que esté en peligro el derecho a la autodeterminación informativa, aún cuando el Estado alegue estos intereses públicos, se demuestre que esa comparación de datos o el procesamiento en concreto sea el único medio idóneo y racional para alcanzar los fines propuestos, de manera que no se haga nugatoria la expectativa de los ciudadanos de que el Estado tendrá también límites en su actividad investigativa⁷⁴.

e. Los requisitos para el ejercicio del Habeas Data

El artículo 75⁷⁵ establece los requisitos para el ejercicio del Ha-

⁷³ Tema que es de singular importancia y que tiene consecuencias políticas y de tutela de derechos fundamentales de una gravedad enorme. El Parlamento Federal Alemán, con los votos favorables de la coalición social cristiana en el poder (CSU-CDU) y del Partido Socialista Alemán (SPD) han dado su visto bueno para la reforma de la Ley del BKA (Bundeskriminalamt) y han creado un marco legislativo para permitir un amplio procesamiento de datos en el ámbito policial, el cual hasta la fecha había tenido sólo un limitado régimen legal. Esta Reforma tiene consecuencias en el ámbito de la tutela de derechos fundamentales, toda vez que con el estandarte de la lucha contra la criminalidad organizada se conceden amplias facultades de investigación mediante el procesamiento de datos personales, pero en realidad el peso de tal investigación y uso masivo de datos personales será usado, en general, para todo el trabajo policial, con muy pocas o nulas posibilidades de control para el ciudadano o para las instituciones encargadas del control como el Datenschutzbeauftragter (Comisionado alemán de la Protección de Datos). Cfr la información sobre la reforma de la BKA-Gesetz en: el Frankfurter Allgemeiner Zeitung del 22 de marzo de 1997).

⁷⁴ Con un análisis de la problemática en Alemania v. Hassemer, *Datenschutz*, op. cit., pp. 37 ss. Sin embargo, matiza esta ausencia del proyecto la existencia del artículo 78 al introducir la posibilidad de eliminar aquellos datos que hayan sido logrados con violación al "debido proceso". Cfr. infra, i.

⁷⁵ Artículo 75. Requisitos. "La petición inicial deberá reunir los siguientes requisitos:

1. El nombre y domicilio de quien interponga el recurso, ya sea persona física o jurídica.
2. La individualización del archivo, listado, registro o banco de datos sobre el que se quiera pedir informes o, en su caso, la institución o persona a cuyo cargo se encuentra.
3. La relación circunstanciada de los datos presuntos en el registro, listado, archivo o banco de datos y el perjuicio que estos pudieran causarle.
4. El requerimiento de la medida por tomar sobre estos datos si se conocieran o denunciaran previamente, sin perjuicio de ampliar, con posterioridad al informe, tal requerimiento.
5. Acompañar la prueba que tuviera a su disposición.
6. La petición en términos claros y positivos.

beas Data. Dos aspectos merecen analizarse con cuidado. Por una parte, en el inciso 2 se exige que el recurrente individualice el archivo, listado, registro o banco de datos sobre el que quiere pedir informes, o la institución o persona a cuyo cargo se encuentra. En este inciso se supone que el afectado conoce donde están sus datos, y, por ello, puede identificar a los encargados del procesamiento de los mismos. Aunque esto es posible en algunos casos de ejercicio del "habeas data", también es posible que el afectado o no sepa más donde están sus datos, no sólo porque el procesamiento de datos no es transparente, sino también porque nunca se le ha pedido su consentimiento para el procesamiento de datos y tampoco se le ha asegurado un efectivo derecho de información preventivo, de manera que él sepa con antelación que sus datos serán objeto de procesamiento electrónico y con qué fin o fines y si eventualmente serán intercambiados. Faltando este derecho a la información sobre el procesamiento, difícilmente podrá el ciudadano cumplir con este requisito exigido en el Proyecto, y probablemente sea el portillo para no admitir muchas demandas de habeas data, aspecto que además tiene sentido por razones de admisibilidad del recurso. Cuando la jurisdicción constitucional tiene tantos expedientes activos como la costarricense, se da el fenómeno que los requisitos de admisibilidad son puntillosamente exigidos y analizados, y podría ser bien la razón para que una gran cantidad de habeas data propuestos por los ciudadanos no cumplan el objetivo que el pre-legislador se ha fijado. En tal caso conviene revisar la eliminación de este requisito y establecer, en su lugar, la necesidad de indicar dónde presumiblemente se piensa que han sido guardados los datos, a fin de tener un punto de partida, y esto sólo en el caso que se sepa su paradero.

En otros países, sobre todo en aquellos donde existen controles preventivos⁷⁶ desde la misma fundación del fichero o banco de datos,

El recurrente deberá expresar cada una de sus peticiones por aparte, y si tiene pretensiones indemnizatorias, deberá exponerlas junto con las razones que las justifiquen, y el daño producido o por producirse.

Deberá decirse si el recurso es interpuesto para efectos del ejercicio de la autodeterminación informativa, o si se trata de derecho al acceso a la información que le concierne. Se consignarán los derechos aparentemente violados o en peligro de ser violados y las razones..."

⁷⁶ Pensamos que difícilmente tendrá el "habeas data" una función preventiva, aún cuando la Exposición de Motivos del Proyecto así lo postule, al menos como una expectativa loable. Cfr. Exposición de Motivos del Proyecto. p. 17.

existe una mayor posibilidad de control sobre el paradero de los datos, ya sea por medio de inventarios frecuentes por parte de una autoridad encargada tanto dentro de la organización como fuera de ella, como es el caso del *Datenschutzbeauftragte* en cada una de las firmas privadas que llevan en Alemania un procesamiento de datos personales cuantioso. Pensamos que en el caso del Proyecto, el mismo fracasará en su objetivo de realizar labores de prevención sobre posibles peligros para la autodeterminación informativa, precisamente porque se ha confiado esta misión a un órgano jurisdiccional que buenamente podrá hacer frente a las demandas planteadas, pero poco o nada podrá hacer por inmiscuirse en un proceso de control que también depende del manejo de ingentes recursos informáticos que éste no posee, así como tampoco el tiempo indispensable para trabajar en una etapa del procesamiento que es tremendamente peligrosa para el ciudadano: la transmisión de los datos⁷⁷.

El Proyecto también exige un requisito que bien puede eliminarse como es el de la necesidad de indicar si el *habeas data* se ejerce para efectos de la tutela "...de la autodeterminación informativa, o si se trata del derecho al acceso a la información que le concierne" al ciudadano. Este requisito no tiene sentido, en primer lugar, porque es posición casi unánime en la doctrina que el derecho a la autodeterminación informativa forma parte de la "*freedom of information*", y que es una forma de su

⁷⁷ Sobre la regulación en la materia en otras legislaciones del mundo v. Kilian Wolfgang, *Persönlichkeitsschutz und grenzüberschreitender Datenverkehr*, en: *Tinnefeld/Philpps/Weis* (Edit.), *Institutionen*, pp. 68 y ss.

⁷⁸ Hassemer cita, por ejemplo, la nueva ley de información sobre el ambiente alemana (*Umweltinformationsgesetz*) que establece un derecho del ciudadano para obtener información de las autoridades encargadas de la protección del ambiente sobre temas relacionados con ésta protección, es en esencia un derecho de acceso que se entiende incorporado en el sentido jurídico de la autodeterminación informativa, la cual, en todo caso, no puede sobrevivir sin un derecho a la información correlativo. El Prof. Hassemer de Francfort del Meno se refiere así de esta manera al tema en cuestión: "La "*Freedom of information*" es el gemelo del derecho a la protección de datos personales y su vecino de enfrente. Esto no debe conducir a interpretar que la relación entre ambos es siempre relajada, bajo ciertos específicos presupuestos institucionales existen ciertas tensiones pre-programadas (por supuesto, no siempre todas las tensiones son paralizantes). Sin embargo, esta comprobación conduce a la necesidad de que el derecho a la información y el derecho a la privacidad sean colocados en condiciones de igualdad y llevados a una correcta concordancia. El derecho a la protección de datos personales sin la "*Freedom of information*" es tuerto. También aquí tendremos que enriquecer y completar nuestra perspectiva en el derecho a la privacidad. El legislador federal ha fundado, ante la suave presión europea, y en el ámbito de la administración del medio ambiente, derechos de información para el ciudadano; y los ha equilibrado con el derecho a la protección de datos personales y con los intereses económicos". Hassemer, *Datenschutz*, op. cit., p. 23.

ejercicio⁷⁸, y, por otra parte, porque podría crear un requisito de admisibilidad, que observado con el detalle con el que suelen ser tratados estos requisitos, cerraría la puerta innecesariamente de la jurisdicción constitucional, haciendo nugatorio el ejercicio mismo del derecho que debe alegarse y que es de naturaleza plural como lo es el derecho a la autodeterminación informativa, como el mismo pre-legislador ha sabido ver en la Exposición de Motivos del Proyecto de Reforma⁷⁹.

f. Sobre la problemática de los datos sensibles y la fase de transmisión de los datos.

El artículo 77⁸⁰ del Proyecto se refiere a los casos en que la Sala Constitucional puede ordenar la suspensión de una transmisión de datos, cuando la misma verse sobre datos sobre los cuales se impugna su confidencialidad o cuando se está tratando de incluir⁸¹ un "dato que parece ser sensible o confidencial". El Proyecto no hace aquí ni siquiera un listado ejemplificativo de los posibles "datos sensibles" lo que deja abierta nuevamente la interpretación⁸².

⁷⁹ Cfr. Exposición de Motivos del Proyecto, pp. 7 y ss.

⁸⁰ "Artículo 77. El segundo efecto del recurso es el de suspensión, y procederá siempre precautoriamente en los siguientes casos:

- a) Cuando el dato está siendo transmitido y se impugna su confidencialidad, debe suspenderse la transmisión o revelación.
- b) Cuando se está tratando de incluir un dato que parece ser sensible o confidencial, debe suspenderse la inclusión.
- c) Cuando la información se impugna por inexacta, falsa o desactualizada, debe suspenderse su transmisión.
- d) Cuando seguir transmitiendo la información o seguirla almacenando pueda causar en el futuro, daños irreparables o los esté causando ilegítimamente..."

⁸¹ No se entiende si "incluir" se refiere aquí a la fase de recogida de los datos o a una eventual inclusión en una transmisión ilícita o no autorizada.

⁸² El artículo 78, inciso b, vuelve a hablar de la "...recolección de datos evidentemente sensibles" y sólo agrega que una eventual eliminación o supresión de los mismos se aplicará cuando "...no exista un fin legítimo para almacenarlos o transmitirlos", lo que de inmediato lleva a analizar cuándo es posible que exista un "fin legítimo" para la recolección y procesamiento de este tipo de datos, los cuales, en general siempre quedan fuera de las posibilidades de cualquier procesamiento, salvo en los casos en que haya un consentimiento expreso del ciudadano, o una obligación legal, pero en cualquier

Ya se ha dicho que sobre el tema de los datos sensibles, la misma doctrina no ha logrado ponerse de acuerdo sobre qué datos forman parte de esta clasificación, problema que surge recién de un aspecto técnico de las nuevas formas de comunicación y procesamiento que han hecho posible que todos los datos, por nimios que sean, tengan significación para un procesamiento dirigido a la conformación de un perfil de personalidad o para una comparación de datos para arrojar conclusiones sobre una persona o un grupo de personas. Debido a ello es que, por ejemplo, el legislador alemán no incluyó una regulación específica de los datos sensibles en la Ley Federal de Protección de Datos (BDSG)⁸³. De hecho, en la legislación sobre datos personales en Alemania es posible detectar una tendencia a prestar una especial atención a los datos y su contexto, no importando su aparente nimiedad⁸⁴.

La reciente Directiva de la Unión Europea del 24 de julio de 1995 en materia de protección de la persona frente al tratamiento de datos personales, y en una tendencia distinta a la seguida por la legislación alemana, en su artículo 8, Abs. 1, prohíbe el procesamiento de determinados datos sensibles a menos que exista un expreso consentimiento del afectado o una expresa facultad legal que permita el procesamiento.

caso no se admiten ficheros o bancos de datos que sean creados exclusivamente para el tratamiento de datos relacionados con la actividad sexual, las creencias religiosas, filiaciones políticas. En cuanto a los datos de salud, o sobre el uso de sustancias alcohólicas o tóxicas, los comportamientos o los hábitos y las características sexuales generalmente pueden ser tratados en ficheros que sean administrados por personas o entidades del ramo de salud y con el propósito único de que tengan un fin terapéutico, debido a su alto valor en este campo. Cfr. en este sentido el texto del Anteproyecto de Ley Colombiana de Protección de Datos, en: Losano, Mario; Pérez Luño, Antonio; Guerrero Mateus, María Fernanda, *Libertad Informática y Leyes de Protección de Datos Personales*, Madrid, Centro de Estudios Constitucionales, 1989, (arts. 20 y 21), pp. 124-125. También el art. 7 y 8 de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de Datos de Carácter Personal, de España (LORTAD).

⁸³ Puede analizarse en este contexto lo expuesto por la BDSG en el § 35 Abs. 2 Nr. 2, que establece que los datos personales deben ser borrados cuando se trata de datos referidos a la condición de salud, a actividades delictivas, contravenciones, así como en lo referido a las convicciones políticas o religiosas, y cuando su exactitud no pueda ser demostrada por el encargado del procesamiento de datos ("speichernde Stelle").

⁸⁴ Cfr. en este sentido, por ejemplo, Ehmann, Horst und Sutschet, Holger, *EU-Datenschutzrichtlinie. Umsetzungsbedarf und Auswirkungen aus der Sicht des Arbeitsrechts*, RDV 1997, p. 9 y ss.

Al ser la Directiva del 24 de julio de 1995 obligatoria para los países de la Unión Europea, será necesario que éstos introduzcan regulaciones específicas para el tratamiento de "datos sensibles", en donde resultaría posible la inclusión de un listado característico pero con carácter de "numerus apertus". En este listado podrían incluirse datos referidos a aspectos de religión, filiación política, escogencia sexual, datos sobre historia clínica, entre otros.

g. El procesamiento de datos personales realizado por la Administración Pública y los particulares

El Proyecto procede, desde nuestro punto de vista correctamente, a no hacer una distinción entre el procesamiento de datos en manos de los particulares o del Estado, lo que hace que esta regulación se acerque al moderno estándar que se pretende alcanzar en el sistema europeo.

La justificación de esta medida puede encontrarse precisamente en que no sólo no debe hacerse una distinción entre el procesamiento "manual" o "automático", ya que basta con que los datos personales reciban una determinada ordenación para facilitar su recuperación, sino porque ha de atenderse al fenómeno de finales de la década de los años 80 y de la presente década de los 90, donde el procesamiento de datos en manos de los particulares tiene un papel decisivo, y ya el Estado no tiene un interés directo en desarrollar bases de datos propias, basta con que tenga acceso a estos acervos en manos de los particulares⁸⁵.

⁸⁵ Recientemente el periodista Armando Mayorga reportó el extraño cobro de 400 colones por mes de una póliza de vida que la compañía de tarjetas de crédito había suscrito para los tarjeta habientes con el INS. En este caso se trata, cómo él lo indica de un cruce de informaciones con la poderosa base de datos de la compañía de crédito, la que permite determinar el número de clientes que estarían dispuestos a suscribir una tal póliza. Sin embargo, el consentimiento del interesado no se toma en cuenta, ni siquiera se le pide que indique los beneficiarios en caso de muerte, simplemente se le deduce automáticamente el monto del pago mensual, que por ser reducido (400 colones mensuales) no provoca en muchos tarjeta habientes protestas. Como el periodista lo comenta, se trata aquí de un ejemplo más del tremendo poder de los particulares en el campo del tratamiento de datos, y de la necesidad de tutela del individuo, sobre todo cuando estos particulares, con el estandarte de la economía de mercado, empiezan a decidir por otros, sin importar su consentimiento. Cfr. Periódico La Nación Digital, <http://www.nacion.co.cr/>, del 1 de julio de 1997, Sección Opinión, Armando Mayorga.

Interesante en este sentido, es que este articulado de Reforma a la Ley de la Jurisdicción Constitucional estaría ampliando la tutela del ciudadano también frente a los eventuales peligros a sus libertades y derechos provenientes de los particulares, lo que generará sin duda una interesante jurisprudencia constitucional de amparo específico (habeas data) frente a particulares, lo que provocará la revitalización de una muy relegada discusión en ámbitos doctrinales y judiciales en Costa Rica.

h. La no especificación de los principios derivados del derecho a la protección de datos en el articulado de la Reforma

El proyecto de reforma, al ser una regulación del "habeas data" y sus extremos, no ha considerado la inclusión de los principios del derecho a la protección de datos⁸⁶. Técnicamente la medida es correcta, sin embargo, y siempre dentro de la línea expresada más arriba, sería conveniente que el proyecto tomara en cuenta la posibilidad de enunciar algunos principios de la protección de datos que resultan esenciales, y que tienen una íntima vinculación con el recurso de habeas data⁸⁷.

⁸⁶ Derechos que también se desprenden de documentos internacionales en la materia como la Convención del Consejo de Europa, del 28 de enero de 1981 (Convención para la Protección de las Personas en lo relativo al tratamiento automático de datos personales), así como las líneas directrices de la OCDE del 23 de setiembre de 1980, en ambos textos se hace referencia los principios aquí comentados del derecho a la protección de datos personales. Cfr. Chirino Alfredo, *Informática y Derecho a la Intimidad. Perspectivas de Política Criminal*, en: *Revista Judicial de Costa Rica*, No. 53, marzo 1991, p. 150, también Lucas Murillo de la Cueva, op. cit., 142-143. Sobre la enunciación de los principios en la LORTAD española, confrontados con la reciente directiva del Consejo de Europa, v. García Beato, op. cit., pp. 35 y ss.

⁸⁷ Flaherty, un autor que se ha dedicado desde 1964 al tema de la privacidad y de la protección de datos, y que ha realizado importantes trabajos comparativos en esta área, nos llama la atención acerca del hecho de cómo en la mayoría de las legislaciones sobre protección de datos no se definen claramente los intereses de la protección, así como los principios de tutela que habrían de ser implementados a fin de evitar o de limitar la vigilancia sobre los ciudadanos. Un problema que parece ser endémico en las legislaciones sobre la materia. Flaherty David H., *Protecting Privacy in Surveillance Societies*, Chapel Hill, The University of North Carolina Press, 1989, p. 377. Esta tendencia bien podría ser evitada en el proyecto, haciendo alusión a un listado de principios, los cuales también podrían orientar la correcta interpretación de los fines de tutela, los cuales, de manera expresa ha señalado el pre-legislador en la exposición de motivos del proyecto.

El derecho a la autodeterminación informativa tiene como base los siguientes principios, los cuales se encuentran hoy consignados en la mayoría de las legislaciones de tutela:

- ◆ el principio de la libertad de decisión del afectado sobre el fin u objetivo del procesamiento de sus datos personales.
- ◆ el principio de transparencia sobre el tipo, dimensión y fines del procesamiento de datos. El afectado debe conocer quién y con qué fines realiza un tratamiento de sus datos personales.
- ◆ el principio de sujeción al fin del procesamiento, para el cual el ciudadano ha dado su consentimiento⁸⁸ a partir de un conocimiento que se le ha facilitado sobre tal fin u objetivo.
- ◆ el principio de división técnica y organizacional entre el procesamiento de datos frente a otros fines de utilización de los datos personales (principio de separación de poderes informativos).
- ◆ el principio de prohibición del procesamiento de datos "a beneficio de inventario" o para almacenarlos con el fin de facilitar la verificación de un tratamiento de datos no autorizado posterior, y la prohibición de la construcción de perfiles a partir del procesamiento de datos personales.
- ◆ el derecho "al olvido" mediante la implementación de reglas de destrucción de los datos personales una vez ha sido cumplido el fin para el que fueron recopilados.
- ◆ el principio de aseguramiento técnico de la realización de los principios jurídicos dirigidos a al tutela del individuo frente al procesamiento de sus datos personales.
- ◆ el principio del control del procesamiento de datos a partir de lugares de procesamiento independientes.

⁸⁸ La nueva Directiva del Consejo de Europa, aparecida a finales de 1995, sobre el tema de la protección de la persona frente al tratamiento de datos, pone un especial énfasis en este principio. Un tratamiento de datos será permitido si la persona ha prestado su consentimiento o si existe una norma legal que lo autorice. Cfr. Werthebach, Eckart, 20 Jahre Bundesdatenschutzgesetz -vom Stiefkind zum Exportmodell, en: Revista Recht der Datenverarbeitung (Alemania) 1997, p. 1 ff.

En adición a estos principios, funcionan además otras reglas que tienen como sentido el potenciar los efectos preventivos que se desprenden de estos principios. Nos referimos, por ejemplo, a las reglas de la anonimidad de los datos, las cuales funcionan para facilitar el procesamiento de datos personales, pero a la vez para proteger al ciudadano de un seguimiento de sus datos mediante la asignación automática de sus datos a su persona mediante características que permitan individualizarlo, como sería un procesamiento, por ejemplo, a partir de su nombre y de un número de identidad. En materia de manejo de datos estadísticos, la regla de la anonimidad tiene un carácter importantísimo.

Junto a la regla de anonimidad funciona también el derecho del ciudadano a rectificar los datos que hayan sido falsificados o alterados o borrados, así como el derecho a una reparación económica de los daños que le hayan sido ocasionados por una destrucción de los datos sin su consentimiento. En consonancia con estos fines de tutela, el derecho a la autodeterminación informativa concede un especial interés al desarrollo de reglas de seguridad del procesamiento, de transparencia y de información de los ciudadanos, a fin de que la aspiración al mantenimiento de la verdad y la transparencia del procesamiento no vayan a declinarse a fin de privilegiar usos ilegítimos de la información a espaldas del ciudadano.

i. Informaciones y debido proceso

El artículo 78⁸⁹ del Proyecto se refiere a la "eliminación y supresión de la

⁸⁹ "Artículo 78: El efecto de la eliminación o supresión de la información o el dato impugnado se aplicará, inmediatamente, en los siguientes casos:

a) Cuando se trate de la recolección de información confidencial con fines de publicación o transmisión a terceros no legitimados para conocerla.

b) Cuando se trate de la recolección de datos evidentemente sensibles y no exista un fin legítimo para almacenarlos o transmitirlos.

c) Cuando la permanencia de los datos haya perdido su razón de ser, por haber transcurrido una prescripción o por ser inútil tal información, a efectos de cumplir con el fin para el que fueron almacenados.

d) En los casos en que figure una información que haya sido obtenida por delito, desviación de poder, por falta o negligencia del informante o del solicitante de la información, por violación del debido proceso o cuando, por conexión, deba eliminarse por haberse declarado ilegal la fuente que la dio a conocer.

En los casos anteriores, la Sala se pronunciará sobre el otorgamiento de posibles daños y perjuicios por las faltas cometidas."

información o del dato impugnado“ en algunos casos especiales. Ya se han comentado algunos de estos casos, pero merece especial referencia el inciso d) del art. 78 que se refiere a los casos en que „...una información haya sido obtenida por delito, desviación de poder, por falta o negligencia del informante o del solicitante de la información, **por violación del debido proceso** (la negrita no es del original) o cuando, por conexión, deba eliminarse por haberse declarado ilegal la fuente que la dio a conocer.“

Este inciso d) abre la puerta para que puedan examinarse por vía del habeas data las posibles lesiones a la autodeterminación informativa que cometan, por ejemplo, las autoridades de la investigación penal cuando, en ejercicio de sus facultades, realicen un procesamiento de datos que no haya sido autorizado de acuerdo a las reglas del debido proceso⁹⁰.

El problema es grave y tiene muchas consecuencias tanto al nivel de la práctica de los órganos de la investigación penal como también a nivel del orden constitucional⁹¹, ya que los ataques de orden informativo son también ataques para los derechos fundamentales, muy especialmente para el derecho a la autodeterminación informativa, toda vez que los datos que son utilizados en las investigaciones pueden provenir, tanto de una

⁹⁰ Reglas que tienen rango constitucional en el artículo 39 de la Carta de 1949 de Costa Rica y que han sido reafirmadas y profundizadas en el fallo de la Sala Constitucional No. 1739-92 (sentencia del debido proceso) de las once horas con cuarenta y cinco minutos del primero de julio de mil novecientos noventa y dos.

⁹¹ Este aspecto constitucional, tanto desde el punto de vista de la salvaguarda del contenido esencial de los derechos fundamentales, como del uso de un determinado medio de prueba dentro de la práctica cotidiana de los órganos del control penal, obliga a referir no a garantías formales (por ejemplo, la intimidad como un derecho formal garantizado) sino a efectivos medios de tutela de los derechos, también frente al sistema penal. El nuevo Código Procesal Penal de Costa Rica (artículo 182) nos enfrenta a esta paradoja en la declaratoria de garantías cuando dice, interpretado a contrario sensu: “A menos que favorezca al imputado, no podrá utilizarse información obtenida mediante la tortura, maltrato, coacción, amenaza, engaño, **indebida intromisión en la intimidad del domicilio**, la correspondencia, **las comunicaciones, los papeles y los archivos privados, ni información que menoscabe la voluntad o viole los derechos fundamentales de la persona**”(la cursiva no es del original). Este artículo, como nos lo recuerda Armijo Sancho, daría opción para que también en la jurisdicción de adultos y juvenil se deje “...sin contenido esencial las garantías que protegen la declaración del imputado, lo mismo que su derecho a la intimidad y el secreto de las comunicaciones...” Armijo Sancho, Gilbert, Justicia Penal Juvenil y Derechos Fundamentales, manuscrito, 1997, p. 11. Quizá el habeas data sea un remedio interesante contra esta filtración grave en el esquema de garantías en favor del imputado, el debate está en todo caso abierto para el momento de la entrada en vigencia de esta normativa procesal en Costa Rica.

unificación de datos de diverso origen (que fueron recopilados con fines distintos a los de una investigación criminal) como también de la utilización de datos que ya habían sido recopilados por las autoridades pero sin seguir los límites o determinaciones propios del derecho a la protección de datos.

Los supuestos son muy variados. Se trata no sólo de la recopilación de datos obtenidos a través de la policía o del ministerio público, quienes tendrían al efecto un verdadero banco de datos de pruebas y de datos personales para efectos de la investigación de delitos⁹², como también obtendrían datos a partir de la unión y comparación de datos de diversas fuentes: fuentes oficiales (registros y oficinas públicas) como también fuentes privadas: agencias de viajes, tarjetas de crédito, llamadas por medio del teléfono celular, observaciones y recopilación de los datos de allí producidos, entre otros. Todas estas recopilaciones y procesamientos de datos son hoy posibles, y para los cuales no existe ni un fundamento legal claro, como tampoco existen reglas que den sentido al ejercicio de un derecho a la protección de datos. En primer lugar, no existen disposiciones que permitan establecer en qué forma se realizará el procesamiento de los datos en sus diversas etapas, no se dice quien podrá ordenar el procesamiento con fines de la investigación, ni tampoco se establecen reglas para la seguridad de los datos, como tampoco plazos a partir de los cuales, ciertos datos, por su sensibilidad deban ser destruidos una vez terminado el proceso para el que fueron ordenados. En segundo lugar, no parece haber límites para la recogida de datos, ya que aquí parece que cualquier ciudadano podría ser considerado para ser objeto de un detallado análisis de sus datos, incluso de aquellos ciudadanos no sospechosos de haber cometido delito, es decir, por ejemplo, personas contacto o personas que sin saber ni de la investigación ni de los objetivos de la recopilación pasan a formar parte de la misma a partir de un hecho casual (un primer contacto con el sospechoso) o por una llamada telefónica o la mera presencia (con otros fines distintos a la visita social al sospechoso) en el apartamento o habitación del sospechoso. Es decir, que el principio

⁹² Se podrían enumerar aquí desde huellas dactilares, estudios genéticos, forenses, psicológicos y psiquiátricos, declaraciones de testigos y de la víctima, etc., hasta pruebas derivadas de escuchas telefónicas y otras intervenciones de las comunicaciones.

de inocencia estaría siendo seriamente lesionado si no se establecen los límites a partir de los cuales las personas pueden ser objeto de una recopilación de datos para el proceso penal.

Por estas razones, la determinación de incluir en el proyecto esta posibilidad de "eliminación de datos" es una herramienta importantísima para que los ciudadanos se protejan frente a posibles lesiones a sus derechos fundamentales producto de la actividad del Estado, incluso en los supuestos en que esté de por medio una investigación de un hecho delictuoso, pero que para lograr los fines de esta investigación se utilicen medios no admisibles o con violación a las reglas de la autodeterminación informativa que también forman parte directa de las reglas del debido proceso, toda vez que incluyen para los ataques informativos la necesidad de resguardar los derechos de defensa, de inocencia⁹³, el principio de culpabilidad y el derecho a ser informado de la incoación de un proceso y las razones del mismo a fin de preparar una defensa técnica.

Un procesamiento de datos que no respete estos derechos, y utilice datos tanto sensibles como no sensibles para los efectos de la realización de perfiles de conducta para demostrar la participación criminal en un determinado hecho, debe ser considerado violatorio del debido proceso. Esto no significa que haya una carta blanca para que los delincuentes se rearmen con la herramienta informática o que estos queden fuera de la acción del Estado producto de haberle atado las manos a las autoridades encargadas de investigar los delitos, sino que significa que también en materia de derecho probatorio, y, sobre todo, cuando se trata de un procesamiento de datos con ese fin, se deben cumplir una serie de reglas y principios que forman parte integral del derecho procesal como derecho constitucional aplicado⁹⁴. El pre-legislador costarricense ha dado un primer paso en este sentido abriendo la posibilidad de utilizar el habeas data para examinar cada caso en que haya ocurrido un procesamiento de

⁹³ Cfr. sobre el principio de inocencia Llobet, Javier, *La prisión preventiva (límites constitucionales)*, San José, Costa Rica, Imprenta y Litografía Mundo Gráfico, 1997, pp. 151 y ss.

⁹⁴ Así lo ha considerado el Tribunal Constitucional Federal Alemán en su sentencia incluida en el Tomo 32 de la edición compilada de sus resoluciones, p. 373 (383), también aparecida en la revista alemana *Neue Juristische Wochenschrift* de 1972, p. 1123. BVerfG 32, 373 (383) NJW 1972, 1123.

datos que produzca una eventual incoación de un proceso, a fin de determinar la realización de los principios constitucionales en juego, y el respeto del acusado, a fin de que este no termine convertido en un objeto de la investigación⁹⁵.

El inciso d) del art. 78 del Proyecto es muy rico en posibilidades, también en lo que se refiere a la "eliminación" del dato cuando por "conexión" resulte que la información haya provenido de una fuente que haya sido declarada ilegal. Este aspecto del Proyecto tanto puede interpretarse positivamente en el sentido de que sea una fuente (banco de datos) cuyo funcionamiento sea ilegal⁹⁶ como también cuando la fuente, aunque legal, haya actuado en violación, por ejemplo, del debido proceso, lo que hace que los datos ofrecidos por la fuente habría de eliminarse o suprimirse, lo que daría la posibilidad de analizar prohibiciones probatorias también en el proceso penal, y utilizar las reglas, hasta ahora empleadas por la jurisprudencia, para ordenar los efectos anuladores que como consecuencia brotan del uso de las pruebas ilícitas.

Otros aspectos quedan sin cobertura en el Proyecto en relación con el "debido proceso" y el uso de datos personales en la administración de Justicia. Por ejemplo, aún quedaría por analizarse los eventuales requisitos que deberían cumplirse para dar seguridad y privacidad a los datos personales que forman parte de los expedientes judiciales, los cuales, muy pronto, y con la tecnología que pronto pondrá en funcionamiento el

⁹⁵ La Sala constitucional costarricense analizó un caso de habeas corpus (V. 445-95, de noviembre de 1995, en recurso planteado por M.Z.S. en favor de C.E.C.C. contra el Juez de Instrucción de Curridabat y el Fiscal J.Ch.G.) en que se solicitaba que unos cassettes en los que constaban unas intervenciones telefónicas probatorias en un asunto de tráfico internacional de estupefacientes no fueran entregados a la prensa y que no se tomaran como prueba para un proceso penal que tenía lugar en los Estados Unidos. La esencia de este recurso era básicamente el ejercicio de las facultades del habeas data, como lo señalan correctamente Fuscaldo y Chavarría. El recurso fue admitido parcialmente, a fin de que datos del proceso penal no pasaran a manos de terceros que no formaban parte de ese proceso, ni que las pruebas fueran utilizadas más allá del proceso penal donde habían sido autorizadas las intervenciones telefónicas. Cfr. Fuscaldo, Gloriana y Chaverri, Alejandra, El Habeas Data en Costa Rica, San José, Costa Rica, Facultad de Derecho, Universidad de Costa Rica, Tesis de Grado para optar al Título de Licenciadas en Derecho, 1995.

⁹⁶ Como el Proyecto no dice cuando se debe estimar que una fuente es "ilegal" debemos suponer que esto resulta del hecho de haber incumplido alguno de los puntos considerados en los artículos 77 y 78, que son precisamente los que dan razón a una actividad del recurrente solicitando la suspensión, eliminación o supresión de un dato.

Poder Judicial⁹⁷, hará posible no sólo la incorporación de los expedientes de manera digital en un equipo central o descentralizado de procesamiento, sino también su consulta de manera remota por vía telemática. Sobre estos aspectos sólo resta reflexionar y tenerlos en cuenta como posibles fuentes de preocupación para el legislador y el ciudadano, ya que el *habeas data*, salvo en aplicación de alguno de los supuestos analizados aquí, poco podrá hacer para brindar la necesaria tutela de la autodeterminación informativa, que en estos casos requiere de otros elementos y de normativas específicas y claras sobre la materia.

j. Aspectos que aún deben de ser considerados en el Proyecto

Sería aconsejable aprovechar la coyuntura para ir un poco más allá, no sólo construir un recurso específico a ser planteado ante la Sala Constitucional para la tutela del ciudadano frente al tratamiento de sus datos personales, sino también establecer una serie de disposiciones que tengan un fin preventivo, y permitan un control técnico constante del tratamiento de los datos personales, así como también de los diversos medios que actualmente se utilizan para recabar datos de los ciudadanos, y que debido a un vacío legal no encuentran en la actualidad un límite razonable, que le dé a los ciudadanos la certeza de que la recogida de sus datos se da dentro de un marco de legalidad.

Esta fase preventiva difícilmente puede ser cumplida por la Sala Constitucional, la cual probablemente entrará a conocer de la problemática una vez que el daño o lesión al bien jurídico se haya verificado. En esta etapa ya todo lo que se haga, probablemente, será tardío, y se restringirá a satisfacer la pretensión concreta del recurrente. El artículo 77, párrafo último del Proyecto, parece darse cuenta de esta problemática, cuando afirma:

⁹⁷ Problema que ya preocupa, por ejemplo, a España, cfr. Alvarez-Cienfuegos Suarez, José María, La protección de los datos personales frente a los tratamientos y ficheros automatizados del poder judicial, en: Agencia de Protección de Datos, Jornadas sobre el Derecho Español de la Protección de Datos Personales, Madrid, 1996, pp. 184 y ss.

*"Según la urgencia del asunto, si se prevé que se pueden causar daños futuros o inmediatos, el magistrado dictará, al recibir el escrito de interposición, la suspensión del acto o mecanismo que permita la transmisión de los datos o la creación de la **central de información en un plazo de veinticuatro horas** (la negrita no es del original) y por todo el tiempo que transcurra hasta la sentencia, esta disposición surtirá efectos sobre todos los registros conexos donde pueda aparecer el dato impugnado. Incurriendo la Sala en responsabilidad civil y hasta administrativa, si por no dictar tal mandamiento, el recurrido sufre perjuicios personales o económicos".*

Antes que nada, no parece claro que intentará el pre-legislador decir cuando se refiere a una "central de información". Tanto puede estarse refiriendo a que la Sala Constitucional tendrá ella que hacerse cargo del tráfico telemático del banco de datos impugnado a fin de garantizar que no se realizará una transmisión de datos ilícita, como también puede referirse a que la Sala Constitucional deberá de ordenar que los bancos de datos que reciban o contengan datos del impugnante suspendan la transmisión o procesamiento del dato impugnado.

En ambos supuestos, creemos que el pre-legislador no puede conceder tales facultades a la Sala Constitucional, por una parte, porque significaría llevar a la ruina a la compañía en concreto que se encargue del procesamiento de datos que esté siendo impugnado, al impedir el normal funcionamiento de su sistema de cómputo, por un tiempo que puede ser realmente largo mientras se decide el recurso, aún cuando el mismo tiene un carácter prioritario en su trámite según el art. 73 del Proyecto, el cual también incluye un plazo no mayor de ocho días hábiles, dentro de los cuales debe sustanciarse el recurso de habeas data. Por otra parte, creemos que la Sala Constitucional no tiene los medios técnicos, ni podrá contar con todos los necesarios a fin de llevar a cabo el primer supuesto que hemos interpretado en el art. 77, es decir, el de constituir una central de información, ya que ni podrá este Tribunal sustituir a la empresa u órgano impugnado en el procesamiento o transmisión de los datos o de centralizar ella el procesamiento de datos en su sede a fin de garantizar que no se van a producir perjuicios al ciudadano⁹⁸.

⁹⁸ Por lo que la posibilidad de declaratorias de responsabilidad civil y administrativa contra la Sala serán muy frecuentes, ante la imposibilidad de garantizar técnicamente por los medios previstos en el art. 77, que se alcance la tutela de la persona frente a eventuales perjuicios personales o económicos derivados del procesamiento del dato o datos impugnados.

Aún cuando se interprete que la Sala Constitucional lo único que hará es hacer un acopio de los datos que se encuentren en los diversos sistemas de cómputo o registros, eso no garantizaría, por ejemplo, que la transmisión del dato ya no se haya dado fuera de las fronteras del país, ya que como se ha dicho, esta transmisión sucede en fracciones de segundo, y no depende de un proceso centralizado de los datos, si no que bien puede producirse desde cualquier lugar, por medio de equipos móviles (lap tops o notebooks) unidos por medio de teléfonos celulares o por INTERNET a un banco de datos parcialmente centralizado, o llevando ellos mismo el acopio total de datos, por ejemplo, en CD-ROM.

Los problemas que refleja este artículo 77 apuntan a los graves dificultades técnicas a los que nos lleva la aceptación del habeas data como único medio, procesal, de tutela de la persona frente al tratamiento electrónicos de sus datos en manos de un Tribunal Constitucional. La garantía del derecho a la autodeterminación informativa tampoco se circunscribe únicamente a la fase de transmisión, sino también a las fases de recogida, almacenamiento y análisis mediante software de los datos.

Resulta necesario, entonces, conceder además facultades de inspección, análisis y autorización a un órgano específico, el cual con una amplia competencia y autonomía funcional y presupuestaria pueda acudir a todos los centros de procesamientos de datos públicos y privados a revisar cómo se realiza el tratamiento de los datos, observar y certificar sus políticas de seguridad, y que tenga la posibilidad de incidir en la peligrosa fase de la transmisión de datos, que dada la actual situación tecnológica puede suceder en cualquier momento, provocando que los datos de las personas sean mercadeados sin ninguna autorización y sin control por parte de los afectados, con los más diversos fines.

Esta forma de control preventivo debe de funcionar, por cierto, con un gran conocimiento técnico, por medio de funcionarios dedicados tiempo completo a ello. Esto es así, ya que el manejo de información involucra hoy en día todo tipo de tecnologías avanzadas, las cuales un órgano judicial, por más buena voluntad, difícilmente podrá evaluar y controlar.

Tomar esta decisión implica, entonces, evaluar la necesidad de crear un sistema de control administrativo, que en la actual tendencia de reducción del Estado casi ninguna posibilidad tendrá de verse hecha una

realidad. Por esa razón, podría pensarse en utilizar herramientas ya existentes para producir esta tutela, como lo sería crear un departamento específico en la Defensoría del Pueblo que se ocupe de estos temas, los cuales son de evidente interés para esta oficina y se refieren directamente a la tutela de derechos del ciudadano.

Esta solución es limitada también, pero sería mucho más abarcadora que la mera aceptación del "habeas data", en la esperanza de que tarde o temprano, con el despertar de la conciencia sobre el problema en la comunidad costarricense se considere la necesidad de ampliar esta tutela mediante la creación de un organismo independiente, con el mayor rango y competencia, independencia funcional y presupuestaria para controlar el tratamiento de los datos personales. Se orientan en este sentido la creación de la figura del Comisionado de la Protección de los Datos en Alemania, de los Registradores de Bases de Datos Públicas y Privadas en Portugal e Inglaterra, de la Agencia de Control del Tratamiento electrónico de Datos de España, del Comisario de la Protección de Datos irlandés y de las Agencia de Informática y Libertades de Francia.

Bien vale la pena estudiar la posibilidad de ampliar esta iniciativa legislativa para crear una ley específica de tutela del ciudadano frente al tratamiento de sus datos personales, la cual le daría al Estado de Derecho costarricense una garantía que lo pondría a la altura de otros ordenamientos jurídicos, que en esta materia nos llevan considerable distancia, así como también permitiría que Costa Rica compita con ventaja en un futuro muy cercano, donde gracias a las condiciones de base con que se cuenta se pueden establecer aquí formas de tratamiento de datos personales de ciudadanos extranjeros, por ejemplo de la Comunidad Económica Europea, creando de esa manera posibilidades de trabajo para la joven industria de la información nacional. Habría ventaja, ya que los países que no ofrezcan garantías similares para la tutela de las personas como las previstas en los estándares de la CE, los cuales ya empiezan a analizarse en el marco de este acuerdo europeo, quedarían fuera del tráfico internacional de datos personales, y por ello impedidos de interactuar de este importante mercado de las próximas décadas⁹⁹. Un mercado donde

se moverán sin duda enormes recursos económicos, los cuales contribuirían a que el país incida con actividades no tradicionales para bien de su propio desarrollo y futuro.

6. Conclusiones Generales

La propuesta de introducir un "recurso específico" para la tutela de la "libertad o intimidad informáticas", tal y como lo postula el Proyecto, resulta ser una manifestación más de la necesidad de llenar un vacío grave en la tutela del ciudadano frente a los riesgos de la moderna sociedad de la información; donde ésta adquiere un valor indudable, abriendo la puerta a nuevas formas de desarrollo humano, pero también a nuevos peligros de construcción de una sociedad panóptica sin lugar para el ocultamiento o para el secreto.

El Proyecto formula, de manera consecuente con la evolución del derecho constitucional en Costa Rica, una ampliación de las competencias de la Sala Constitucional, y utilizando el espejo del "habeas corpus" ofrecer un proceso sumario y expedito para analizar posibles lesiones a la autodeterminación informativa.

A pesar de que la idea está bien orientada, presenta dos graves problemas, uno de ellos de orden práctico, y del otro, de orden tecnológico. En el primer orden de problemas, resulta necesario señalar que el actual volumen de trabajo de la Sala Constitucional costarricense es enorme, lo que la ha llevado casi a colapsar, y a generar preocupación en la doctrina y en el legislador y en los mismos jueces constitucionales acerca del futuro de esta Sala, que ha tenido un papel tan importante en la vivencia activa del Estado de Derecho en Costa Rica, por otra parte, al constituir

⁹⁹ Molina Mateos acota en este contexto que la distancia entre los países que cuentan con tecnología para procesar la información y aquellos que sólo pueden recibirla y consumirla, se está haciendo cada vez más grande, eso sin contar los impedimentos tecnológicos que tienen muchos otros para siquiera acceder la información y utilizarla. Aún cuando el principio de la libre circulación de los datos está recogido en diferentes normativas (verbigracia: Resolución del Consejo de Ministros de la CEE de 1971), este principio sólo parece tener vigencia para los países tecnológicamente más avanzados. La información es hoy, además de un instrumento de poder, "...un imperativo de soberanía" Cfr. Molina Mateos, José María, Seguridad, información y poder, Madrid, INCIPIT Editores, 1. Edición, 1994, p. 21.

el "habeas data" como una "acción de amparo" se corre el riesgo, como lo afirman Altmark y Molina para el caso argentino, de desvirtuar la finalidad del instituto. En el orden de problemas tecnológicos habría que mencionar que el Proyecto olvida que no son con frecuencia los "datos finales" y su manejo los que generan peligros al ciudadano, sino también las diversas formas de recopilación y procesamiento y transmisión de la información. En este sentido, las diversas experiencias del derecho comparado demuestran que el éxito de una regulación depende tanto de una consideración de las diversas fases del tratamiento de los datos, como de los ámbitos específicos en que el tratamiento de datos personales se desarrolla.

Al carecer el Proyecto, por su tendencia hacia el habeas data, de una consideración de estos aspectos tecnológicos - los que por otra parte son decisivos - lleva a limitar ya en sus inicios, y de manera peligrosa, las posibilidades de tutela que podrían obtenerse, sobre todo si se toma en cuenta el desarrollo de la aplicación de las tecnologías de comunicación e información en Costa Rica.

Dentro de las limitaciones que habría que señalar, es que resulta evidente que el Proyecto parte de que el ciudadano es quien se da cuenta de la lesión, quien ha de ofrecer "prueba de cargo", referencia de los funcionarios públicos o de los particulares que han realizado el procesamiento, así como una descripción del "hecho u omisión" que motiva el "habeas data". Estos requisitos que resultan obvios ante el planteamiento de recursos judiciales y que tienen sentido dentro del contexto de las lesiones a derechos fundamentales, que son materia de todo Tribunal Constitucional, son totalmente contradictorios con la "realidad" del procesamiento de los datos personales.

La evolución del derecho comparado presenta gran número de ejemplos de cómo será la estructura futura de las formas de tutela del derecho a la autodeterminación informativa: preventiva más que reactiva, dirigida a potenciar los derechos de información del ciudadano, la utilización de órganos independientes y con capacidad técnica para contrarrestar los avances vertiginosos de la tecnología de la información; así como también el desarrollo de leyes específicas en los diversos campos en que el procesamiento de datos personales incide.

La idea de tutela parece, además, orientada a una posible acción preventiva del Tribunal Constitucional, aún cuando el artículo 77, de manera muy optimista, aunque tímida se refiere a diversas fases del procesamiento, donde teóricamente podría funcionar preventivamente la acción de la Sala Cuarta. Resulta, no obstante, casi seguro que la Sala Constitucional no podrá actuar preventivamente, primero, porque el procesamiento de datos se desarrolla de manera tan vertiginosa y con medios tecnológicos tan veloces y eficientes, que haría imposible una actuación preventiva de este alto órgano jurisdiccional, el cual además está ocupado de otras importantes tareas, las cuales tampoco debe descuidar. De otro lado, resulta, que una ausencia casi absoluta de determinaciones legales y reglamentarias sobre „seguridad de los datos“; "derechos de información del afectado"; y sobre requisitos en cuanto a la "necesariedad" y "apego a los fines del procesamiento", muy difícilmente podrá alegarse con éxito lesiones o posibles ataques informativos a los derechos fundamentales que se pretenden tutelar.

Estas materias, que suelen ser objeto de una ley general de protección de la persona frente al procesamiento de datos personales, no están presentes en el Proyecto, ni tienen por qué estarlo por el tipo de tutela escogida. Tampoco se analiza de qué manera se podrá observar el "interés legítimo" o los "intereses públicos" en el procesamiento de datos personales, como sucede, por ejemplo, en el tratamiento de datos personales en el marco del proceso penal.

Debe de tomarse en cuenta que el "habeas data" por sí mismo es únicamente una garantía procesal, es decir, una forma de tutela de un derecho fundamental a través de un procedimiento, lo que tiene como punto de partida, que el derecho fundamental está claramente planteado, y que los contornos de la tutela son prístinos. Estos dos últimos aspectos no parecen tan claros en el proyecto de reforma, primero porque la misma se concentra a crear y organizar la tutela y, en segundo lugar, porque el lugar para una determinación sobre el derecho a tutelar sería en una ley específica y, quizá, en una eventual incorporación constitucional del derecho del ciudadano a ser protegido frente al tratamiento de sus datos personales¹⁰⁰.

¹⁰⁰ Al respecto v. Simitis, Spiros, Zur Aufnahme der "informationellen Selbstbestimmung" in das Grundgesetz, Stellungnahme gegenüber der Gemeinsamen Verfassungskommission des Bundestages und des Bundesrates, Krit V (Alemania) 1993, pp. 46 y ss.

La información se ha convertido en un valor de cambio en la actual sociedad tecnológica, ella permite no sólo alcanzar muchas metas que el Estado Social se veía imposibilitado de cumplir con eficiencia, como también ha permitido influir en diversas formas de interacción entre los ciudadanos, muy especialmente en su comunicación. Es por ello que resulta necesario abrir un debate nacional para crear conciencia sobre el problema.

Junto al derecho a la información y a ser informado, cobra una especial importancia hoy en día el derecho a la intimidad

El manejo de la información, su tratamiento y transmisión se han convertido hoy en día, junto con las tecnologías que hacen posible esto de una manera rápida y confiable, en las actividades económicas de mayor crecimiento, y sin duda, cumplirán un papel determinante en la forma en que los ciudadanos realicen muchas de sus actividades cotidianas.

Y será sin duda la que determinará el futuro y el desarrollo del mundo, muy especial el de los países de nuestro continente, los cuales están enfrentados en este momento a un dilema enorme provocado por las nuevas interacciones del mercado y el fortalecimiento de tendencias encarnizadas que forma parte de toda declaración de derechos en una sociedad democrática, así como el derecho a la intimidad, que en nuestra Constitución Política, tiene, al menos desde la perspectiva del texto formal, una relación inescindible con la libertad.

En efecto, la tutela de la intimidad es uno de las garantías más importantes del ciudadano, la cual adquiere con el desarrollo de la llamada "sociedad de la información" una relevancia todavía más señera, ya que las herramientas de la moderna tecnología hacen posible, no sólo plantear las bases para un desarrollo más integral de la persona y alcanzar algunos sueños democráticos, como lo es la posibilidad de que cada ciudadano se interese por los asuntos públicos y pueda intervenir directamente en las decisiones que puedan afectar sus derechos, sino que también engendran graves peligros, ya que facilitan el manejo, organización y comparación de una gran cantidad de datos sobre los ciudadanos, los cuales pueden ser así utilizados para controlarle y limitar sus ámbitos de libertad.

En un trabajo publicado hace algunos años en Costa Rica, se ha sostenido que la utilización del recurso de amparo para tutelar al individuo frente a posibles abusos en el tratamiento de sus datos personales es un medio solamente temporal para alcanzar dicha tutela¹⁰¹. Por el carácter tan técnico de esta materia, y tomando en cuenta que los riesgos para el ciudadano se presentan en todas las etapas del procesamiento de los datos, desde que se recopilan hasta que eventualmente se transmiten, el recurso de amparo revela muchas limitaciones, sobre todo que la reacción judicial puede perfectamente producirse cuando los daños para el derecho fundamental ya no pueden ser reparados, o cuando la mera exhibición de los datos o la imposición de una indemnización no realice el objetivo esencial de la tutela, como la que pretende este proyecto de reforma legislativa. Resulta, por ende, necesario, explorar la posibilidad de una tutela ampliada por medio de una ley específica que tome en cuenta los aspectos concretos del derecho a la autodeterminación informativa, como punto de partida en el camino hacia una tutela eficiente del ciudadano frente al tratamiento de sus datos personales.

El proyecto nos pone ante la disyuntiva de escoger al "habeas data" como un primer paso en el desarrollo de formas de tutela más eficientes, o de trascender aún más y formular una ley para la tutela de la persona frente al tratamiento automatizado de sus datos personales. El primer camino nos hace guardar la esperanza de que como ciudadanos podemos utilizar el "habeas data" como herramienta preliminar para forjar conciencia sobre la importancia de esta tutela y para ganar algunas batallas en el movedizo campo tecnológico. El segundo camino, nos obliga a reflexionar acerca de la necesidad de herramientas preventivas que se opongan a los riesgos en la misma etapa en que estos no se han verificado, y de instrumentos legislativos que contribuyan a custodiar las trincheras en donde el procesamiento de datos ha de permitirse por razones de interés colectivo y social, pero con los límites propios de un estado de derecho. Parece que la coyuntura política, social y económica es más proclive a una solución de compromiso, momentánea y esperanzadora, que acepta al habeas data como remedio procesal, en manos de la Sala Constitucional, y con el ropaje del recurso de amparo. Esta solución es interesante pero

¹⁰¹ Chirino, *Informática*, op. cit., pp.149 ss.

quizá demasiado limitada. En todo caso, debemos participar activamente en la discusión de estos problemas, de informarnos de lo que está sucediendo, ya que en pocos momentos de la historia constitucional del país se habrán debatido problemas tan trascendentales para nuestro proyecto político como con la discusión y eventual aprobación de este proyecto de reforma a la Ley de la Jurisdicción Constitucional. Costa Rica revela con esta propuesta una particular madurez en su sistema de tutela de derechos fundamentales, y continua por el camino vigoroso y dinámico iniciado con la creación de la misma Sala Constitucional y posteriormente de la institución de la Defensoría de los Habitantes. La propuesta ahora de un recurso para ejercer el derecho a la libertad informática complementa las garantías de cara al siglo venidero, coyuntura profundamente marcada por la impronta tecnológica y sus promesas.

Si escogemos el segundo camino, es decir, el camino hacia una ley de tutela completa y detallada, quizá nos prepare de una manera más clara y definitiva para definir las trincheras en la lucha constante por la realización y efectividad de nuestros derechos fundamentales. El ciudadano tiene la palabra en esta fundamental época en donde sus derechos y libertades ceden terreno en la búsqueda de quimeras simbólicas, la mayor parte de las veces hasta sin legitimación en el proceso de su discusión. La libertad informática es una libertad tan esencial como la libertad de tránsito o de movimiento, muy especialmente en una sociedad que pone un énfasis tan contundente en el tráfico de datos personales. No en vano se ha dicho, que hay una relación de proporcionalidad directa entre el grado de democracia de un país y el número de informaciones que circulan en ella. En esa misma medida el grado de democracia puede verse en peligro si esas informaciones son utilizadas para reducir al ciudadano a un mero objeto de este trueque. Es ahora donde tenemos la oportunidad de afianzar espacios de libertad, no la desperdiciemos, sobre todo ahora que las aguas están tranquilas y hay espacio para la reflexión y el actuar ponderado. Después puede ser demasiado tarde.

7. Apéndice

A continuación se incluye nuestra propuesta de modificación del Proyecto del Diputado Urcuyo enviada a la Comisión Legislativa encargada de la redacción de la Reforma a la Ley de la Jurisdicción Constitucional para introducir el recurso de hábeas data en Costa Rica. Una versión modificada del proyecto del Dr. Urcuyo ha incluido, en gran parte, las modificaciones sugeridas¹⁰².

Propuesta de Modificación del articulado

Si se mantiene la propuesta de redactar una modificación a la Ley de la Jurisdicción Constitucional para introducir el Habeas Data en Costa Rica, en lugar de redactar propiamente una Ley de Protección de Datos, la cual resultaría más amplia y con un efecto de tutela mayor, el proyecto debería sufrir, según nuestra perspectiva, las siguientes modificaciones:

Artículo 1.- Adiciónase un nuevo Capítulo IV, denominado "Del Recurso de hábeas data", al título III de la Ley de la Jurisdicción Constitucional, Ley No. 7135, del jueves 19 de octubre de 1989. Asimismo, se modificará la numeración de los artículos siguientes.

Artículo 71. **Objeto del Recurso.** El recurso de hábeas data tiene como objeto realizar una protección de carácter procedimental del derecho del ciudadano a su intimidad y libertad informática en el contexto del tratamiento de sus datos personales.

Artículo 72. El recurso de hábeas data podrá plantearse en los siguientes casos:

a) toda persona física o jurídica, podrá plantear el recurso de hábeas data con el fin de conocer lo que conste sobre sí misma o sobre sus bienes, en registros, archivos, listados o bancos de datos, sean manuales, mecánicos, electrónicos o informatizados, públicos o privados,

¹⁰² Ver Expediente legislativo.

- b) la pretensión del recurso de habeas data también puede consistir en solicitar información sobre la finalidad a que se destinarán los datos personales que han sido recogidos, así como también sobre su destino final, y sobre el eventual entrega de los datos personales a otros lugares de procesamiento de datos distintos al del lugar que en primera instancia realizó la recogida de los datos.
- c) mediante el recurso de hábeas data podrá requerirse la rectificación, actualización, inclusión, confidencialidad o cancelación inmediata de los datos personales en poder del lugar de tratamiento de los datos público o privado.
- d) procederá el recurso de hábeas data también para solicitar informaciones que han sido declaradas secreto de Estado. Para efectos de la aplicación de esta norma, secretos de Estado son los asuntos de tramitación de carácter diplomático o que se refieran a las operaciones de seguridad nacional pendientes.
- e) podrá plantearse el recurso de hábeas data en aquellos casos en que haya sido lesionado alguno de los principios relacionados con el procesamiento de datos personales descriptos en el artículo 73.

Artículo 73. Principios del tratamiento de datos personales. El tratamiento de datos personales, tanto en el ámbito privado como público, deberá respetar y seguir los siguientes principios:

- a) Principio de calidad de los datos. Sólo se podrán recoger datos de carácter personal para su tratamiento o para someterlos al mismo, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas para las que se hayan obtenido.
- b) Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades distintas de aquellas para las que los datos hubieran sido recogidos.
- c) Los datos personales que se consignen en un determinado registro informatizado o manual han de ser exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado.
- d) Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados.
- e) Los datos de carácter personal han de ser procesados de manera que sea posible el acceso a los mismos por parte del afectado.

- f) No será permitida la recogida de datos por medios fraudulentos, desleales o ilícitos.
- g) El afectado deberá recibir información acerca del hecho del tratamiento de sus datos personales, de los objetivos o fines de dicho tratamiento, así como de los derechos que le competen de acuerdo a esta ley para acceder los datos que sobre su persona se encuentren consignados en el banco de datos, así como de quién o quiénes realizarán el tratamiento de datos y de cómo podrá hacer ejercicio de su derecho de acceso y revisión de los datos.
- h) el tratamiento automatizado de datos personales requerirá del consentimiento del interesado, salvo que la Ley disponga otra cosa. Sin embargo, no será necesario este consentimiento en los casos de datos de carácter personal que han sido recogidos a partir de fuentes accesibles al público o cuando se recojan para fines de la administración pública en el marco de sus competencias legales, o cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y dichos datos sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

Artículo 74. Perfiles de Personalidad. El afectado podrá impugnar mediante la incoación del recurso de hábeas data los actos administrativos o las decisiones de carácter particular que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o de su personalidad.

Artículo 75. Trámite prioritario. El recurso de hábeas data recibirá un trámite prioritario sobre el recurso de amparo y deberá ser resuelto en un plazo no mayor a ocho días hábiles.

Artículo 76. Legitimación. El recurso podrá ser interpuesto por:

1. La persona física.
2. Los herederos del difunto: ascendientes y descendientes, los colaterales hasta el cuarto grado de consanguinidad, el cónyuge por los derechos del difunto

3. Las personas jurídicas.
4. El Defensor de los Habitantes, y
5. Las asociaciones representativas de los habitantes, por actos de discriminación.

Artículo 77. **Requisitos.** La petición inicial deberá reunir los siguientes requisitos:

1. El nombre y domicilio de quien interponga el recurso, ya sea persona física o jurídica.
2. Una indicación de cuál es el dato o información de carácter personal que se desea controlar mediante el ejercicio del hábeas data, así como una relación circunstanciada del daño o perjuicio que el tratamiento automatizado le ha causado o pueda causarle.
3. Identificación de la persona, oficina o institución que realizó el tratamiento de datos personales, y de la forma en que se realizó la recogida de la información. En caso de que se conozca el lugar donde se conservan los datos u informaciones de carácter personal objeto de este recurso, podrá incluirse una referencia del lugar o lugares probables donde se encuentran.
4. Indicación de qué tipo de efectos se esperan de la resolución que da acogida al recurso de hábeas data. Este requerimiento podrá ampliarse con posterioridad a la presentación del recurso.
5. Acompañar la prueba que tuviera a su disposición.
6. La petición ha de ser redactada en términos claros y precisos.
7. Las pretensiones habrán de indicarse por aparte, y si existe una pretensión indemnizatoria, habrá de indicarse en qué consiste el daño o perjuicio, así como la prueba que permita apreciar su cuantía. En los casos en que no se conozca con anterioridad los daños o perjuicios que

han sido ocasionados con el procesamiento de los datos personales, los mismos podrán ser después reclamados en la jurisdicción correspondiente mediante el proceso de ejecución de sentencia.

Para los efectos de este artículo, se estará a lo dispuesto en los artículos 35, 36 y 38 de la presente ley.

Artículo 78. Efecto de Exhibición. El primer efecto del recurso será el de exhibición, el cual podrá ir acompañado del de certificación, en caso de ser solicitado por la parte interesada. Este consiste en dictar una medida para que determinado dato o información de carácter personal pase al conocimiento del afectado. En cualquier caso, la Sala tendrá acceso a la información que sea objeto del recurso, así como a cualquier otra que considere conveniente para el dictado de la resolución, aún cuando se trate de datos confidenciales de cualquier tipo.

Artículo 79. Efecto de Suspensión. El segundo efecto del recurso es el de suspensión, y procederá siempre en carácter precautorio en los siguientes casos.

- a) Cuando el dato está siendo transmitido y se impugne su confidencialidad, deberá suspenderse la transmisión o la revelación del dato.
- b) Cuando se trate de la inclusión de un datos personales que revelen, entre otros, la ideología, religión, creencias, filiaciones políticas, origen racial, salud o la vida sexual de la persona deberá suspenderse su inclusión, hasta tanto se determine que hubo un consentimiento válido del afectado en dicho tratamiento.
- c) Cuando la información se impugna por inexacta, falsa o desactualizada, debe suspenderse su transmisión.
- d) Cuando seguir transmitiendo la información o seguirla almacenando pueda causar en el futuro, daños irreparables o los esté causando ilegítimamente.

Según la urgencia del asunto, y tomando en cuenta los efectos económicos y materiales que pueda tener la medida sobre el tratamiento de los datos que realiza el responsable del fichero, el magistrado dictará, al recibir el escrito de interposición, la suspensión del acto de transmisión de los datos. En caso de que la información o el dato hayan sido efectivamente transmitidos, o exista dicha posibilidad, el magistrado structor deberá pedir una indicación del encargado del fichero de los lugares donde el dato o información impugnados han sido transmitidos.

En caso de que la fase de transmisión de los datos personales haya sido concluida deberá de solicitarse también la suspensión del posterior tratamiento de esos datos al lugar o lugares de tratamiento que hayan recibido la información o el dato impugnados.

Artículo 80. Efecto de Eliminación o Supresión. El efecto de eliminación o supresión de la información el dato impugnado se aplicará, inmediatamente, en los siguientes casos :

- a) Cuando se trate del tratamiento de información confidencial con fines de publicación o transmisión a terceros no legitimados para conocerla.
- b) Cuando se trate del tratamiento de datos evidentemente sensibles y no exista ni consentimiento expreso del interesado o un fin legítimo para realizar sobre ellos un tratamiento.
- c) Cuando la permanencia de los datos en el fichero respectivo haya perdido su razón de ser, por haber transcurrido el plazo de prescripción previsto en la ley para el caso respectivo o cuando se haya cumplido el fin para el cual fueron tratados.
- d) En los casos en que figure una información que haya sido obtenida por delito, desviación de poder, por falta o negligencia del informante o del solicitante de la información, por violación a las reglas o principios del debido proceso o cuando, por conexión, debe eliminarse por haberse declarado ilegal la fuente que la dio a conocer.

En el caso del inciso d) anterior podrá solicitarse, en los casos que el dato impugnado figure como elemento probatorio en un proceso judicial incoado en contra del afectado, que el mismo no sea utilizado como prueba en contra de éste, por haberse lesionado los derechos y garantías que dan sentido al recurso de hábeas data.

En los casos anteriores, la Sala condenará a la persona o entidad responsable del agravio al pago de los daños y perjuicios sufridos por el afectado.

Artículo 81. Definiciones. A efectos del recurso de hábeas data se entenderá por:

Datos Personales: cualquier información concerniente a personas físicas o jurídicas identificadas o identificables.

Tratamiento de datos: son las operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Responsable del Fichero: Persona física o jurídica, de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento.

Afectado: Persona física o jurídica titular de los datos que sean objeto del tratamiento automatizado o manual.

Artículo 82. Para efectos de devolver la situación al estado anterior o menos perjudicial, se estará a lo dispuesto en los artículos que van desde el 51 hasta el 56 de la presente ley.

Artículo 2. Rige a partir de su publicación.

8. Bibliografía

Altmark, Daniel Ricardo y Molina Quiroga, Eduardo, Protección de Datos Personales y Reforma Constitucional, en: Informática y Derecho, Extremadura, España, UNED, Actas del II Congreso Internacional de Informática y Derecho, v. II, 12-15; 13-14, 1996, pp. 1237 ss.

Alvarez-Cienfuegos Suarez, José María, La protección de los datos personales frente a los tratamientos y ficheros automatizados del poder judicial, en: Agencia de Protección de Datos, Jornadas sobre el Derecho Español de la Protección de Datos Personales, Madrid, 1996, pp. 179 y ss.

Armijo Sancho, Gilbert, Justicia Penal Juvenil y Derechos Fundamentales, manuscrito, 1997.

Bölsche, Jochen (Hrsg.), Der Weg in der Überwachungsstaat, Reinbeck bei Hamburg, Rowohlt Taschenbuch Verlag, 1979.

Bühl, Achim, Cybersociety: Mythos und Realität der Informationsgesellschaft, Köln, Papyrossaverlag, 1996.

Cerqueira Leite Seelander, Airton, Democratização pelos "Mass Media"?- O direito de ser informado e os limites fáticos à sua plena eficácia, en: Revista da Faculdade de Direito, Universidade de São Paulo, Brasil, v. 83, ene-dic 1988, pp. 318 ss.

Cohen, Frederik, Protection and Security on the Information Superhighway, New York, Chichester, Brisbane, Toronto, Singapore, John Wiley & Sons, 1995.

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.

Chirino, Alfredo, Informática y Derecho a la Intimidad. Perspectivas de Política Criminal, en: Revista Judicial de Costa Rica, No. 53, marzo de 1991, pp. 149 ss.

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, (setiembre de 1997).

da Silva Velloso, Carlos Mário, As novas garantias constitucionais: O mandado de segurança coletivo, o Habeas Data, o Mandado de Injunção e a Ação popular para defesa da moralidade administrativa, en: Fidelis Dos Santos, Ernane, Atualidades Jurídicas, Belo Horizonte, Brasil, 1993, pp. 120 ss.

da Silva Filho, Artur Marques, Comentários a Constituição Federal, Saraiva, Brasil, 1991.

da Silva Filho, Artur Marques, "Habeas Data" Remédio heróico ou inócuo, en: RT 649, noviembre de 1989, pp. 220 ss.

Damm, Renate, "Medienprivileg" im Spannungsfeld von Informationsfreiheit und Datenschutz, en: Tinnefeld/Philipps/Weis (Edit.), Institutionen, pp. 131 y ss.

Davara Rodríguez, Miguel Angel, De las Autopistas de la Información a la Sociedad Virtual, Pamplona, Editorial Aranzadi, 1996.

Dordick, Herbert y Wang, Georgette, The Information Society. A retrospective View, Newbury Park, London, New Delhi, Sage Publications, 1993.

Dronsch, Gerhard, Nochmals: Datenschutz in der Informationsgesellschaft, en: ZRP (Alemania), 1996, pp. 206 ss..

Ehmann, Horst und Sutschet, Holger, EU-Datenschutzrichtlinie. Umsetzungsbedarf und Auswirkungen aus der Sicht des Arbeitsrechts, en: RDV (Alemania) 1997, pp. 3 y ss.

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.

Fallas Vega, Elena, Informe Jurídico sobre el Proyecto de Ley: „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, Expediente No. 12827.

Fiedler, Herbert, Informationelle Garantien für das Zeitalter der Informationstechnik, en: Tinnefeld/Philipps/Weis, Institutionen, pp. 147 ss.

Flaherty, David H., Protecting Privacy in Surveillance Societies, Chapel Hill, The University of North Carolina Press, 1989.

Frossini, Vittorio, Hacia un derecho de la información, en: Informática y Derecho, Extremadura, España, UNED, No. 12-15; 13-14; 1996, pp. 809 y ss.

García Beato, María José, Principios y derechos en la Ley Orgánica 5/1992, de 29 de octubre, y en la Directiva 95/46 CE, en: Agencia de Protección de Datos, Jornadas sobre el Derecho Español de la Protección de Datos Personales, Madrid, 1996, pp. 35 y ss.

Garstka, Hansjürgen, Informationelle Selbstbestimmung- ein Menschenrecht?, en: Heymann, Thomas (Edit.), Informationsmarkt und Informationsschutz in Europa: rechtliche Fragen, europäische Harmonisierung/ im Auftrag der Deutschen Gesellschaft für Recht und Informatik e. V. , Köln, Verlag Dr. Otto Schmidt KG, 1995,

Gräf, Lorenz, Privatheit und Datenschutz. Eine soziologische Analyse aktueller Regelungen zum Schutz privater Bereiche auf dem Hintergrund einer Soziologie der Privatheit, Köln, Diss 1993.

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

- Hassemer, Winfried, Über die absehbare Zukunft des Datenschutzes, KJ (Alemania) 1996, pp. 99 y ss.
- Häberle, Peter, Verfassung als öffentlicher Prozeß. Materialien zu einer Verfassungstheorie der offenen Gesellschaft, Berlin, Duncker und Humblodt, 2. Edición aumentada, 1996.
- Kilian Wolfgang, Persönlichkeitsschutz und grenzüberschreitender Datenverkehr, en: Tinnefeld/Philpps/Weis (Edit.), Institutionen, pp. 63 y ss.
- Leuthardt, Beat, Leben on Line. Von der Chipkarte bis zum Europol-Netz: Der Mensch unter ständigem Verdacht, Reinbeck bei Hamburg, Rowohlt Taschenbuch Verlag.
- Lippmann, Ernesto, O Habeas Data visto pela doutrina e interpretado pelos Tribunais", en: Revista dos Tribunais, Brasil, enero de 1996, v. 723, p. 117.
- Llobet, Javier, La prisión preventiva (límites constitucionales), San José, Costa Rica, Imprenta y Litografía Mundo Gráfico, 1997.
- Martín Pallín, José Antonio, Constitucionalidad del Número de Identificación único, en: Agencia de Protección de Datos, Jornadas sobre el Derecho Español de la Protección de Datos Personales, Madrid, 1996, pp. 56 y ss.
- López Fuscaldó, Gloriana y Chaverri Alvarez, Alejandra, El Habeas Data en Costa Rica, San José, Costa Rica, Facultad de Derecho, Universidad de Costa Rica, Tesis de Grado para optar al Título de Licenciadas en Derecho, 1995.
- Losano, Mario, Das italienische Datenschutzgesetz, en: Revista Computer und Recht (Alemania), Nr. 5 de 1997, pp. 308 ss.
- Lucas Murillo de la Cueva, Pablo, El Derecho a la Autodeterminación Informativa, Madrid, Tecnos, 1990.
- Molina Mateos, José María, Seguridad, información y poder, Madrid, INCIPIT Editores, 1. Edición, 1994.

Nusdeo, Marcos y Folgosi, Rosolea, "Habeas Data", en: RDP-87, Brasil, pp. 90 ss.

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 Demokratie, Frankfurt am Main, Suhrkamp, 1. Edición, 1979, pp. 50 y ss.

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, pp. 179 y ss.

Schmitt Glaeser, Walter, Schutz der Privatsphäre, en: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts, Heidelberg, v. VI, 1989, pp. 41 ss.

Scholz, Rupert y Pitschas, Rainer, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, Berlin, Dunker und Humblot, 1984.

Simitis, Spiros, Virtuelle Präsenz und Spurenlosigkeit - Ein neues Datenschutzkonzept, en: Krit V (Alemania) 1996, pp. 99 ss.

Simitis, Spiros, Zur Aufnahme der "informationellen Selbstbestimmung" in das Grundgesetz, Stellungnahme gegenüber der Gemeinsamen Verfassungskommission des Bundestages und des Bundesrates, en: Krit V (Alemania) 1993, pp. 46 y ss.

Simitis, Spiros, Von der Amtshilfe zur Informationshilfe.

Informationsaustausch und Datenschutzerfordernissen in der 6ffentlichen Verwaltung, en: NJW (Alemania) 1986, pp. 2795 ss

Simitis/Dammann/Geiger/Mallmann/Walz, Kommentar zum Bundesdatenschutzgesetz, Baden-Baden, Nomos Verlags-gesellschaft, 4. Edici6n totalmente revisada, 1992.

Staff, Ilse, 6ffentlichkeit als Verfassungsprinzip, ZRP (Alemania), pp. 384 y ss.

Stegbauer, Christian, Euphorie und Ern6chterung auf der Datenautobahn, Frankfurt/Main, Dipa, 1996.

Tinnefeld, Marie-Theres; Philipps, Lothar; Weis, Kurt (Edit.), Institutionen und Einzelne im Zeitalter der Informationstechnik, M6nchen; Wien, R. Oldenbourg Verlag, 1994.

Wegel, Wolfgang, Presse und Rundfunk im Datenschutzrecht, Frankfurt am Main, Peter Lang, 1995.

Weis, Kurt, Die Informationsgesellschaft: Zum Wandel der Menschenbilder unter neuen Technologien, en: Tinnefeld/Philipps/Weis (Edit.), Institutionen und Einzelne im Zeitalter der Informationstechnik, M6nchen; Wien, R. Oldenbourg Verlag, 1994, pp. 25 ss.

Werthebach, Eckart, 20 Jahre Bundesdatenschutzgesetz -vom Stiefkind zum Exportmodell, en: Revista Recht der Datenverarbeitung (Alemania) 1997, p. 1 ff.