

TUTELA CONSTITUCIONAL DEL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA EN COSTA RICA*

MARVIN CARVAJAL PÉREZ[†]

INTRODUCCIÓN:

La sociedad de la información ha acortado el ya limitado *ámbito de intimidad de las personas*, permitiendo que los aspectos más privados de su vida sean compilados en grandes bases de datos, transferidos a cualquier parte del mundo en pocos segundos y usados en las más diversas formas. Si hace tan sólo unas cuantas décadas la privacidad podía ser asegurada protegiendo el domicilio y las comunicaciones escritas y telefónicas de las personas, hoy en día se requiere mucho más. En este campo, el avance tecnológico debe estar acompañado (y cuando sea posible precedido) por la consolidación de una regulación comprensiva y eficaz.

Cada país ha encarado en forma diversa el grave reto que plantea el *acelerado progreso de las tecnologías informáticas y la necesaria protección de los derechos de sus habitantes*. Así, desde naciones que han apostado por una rigurosa regulación estatal (caso de los países europeos) hasta otros que han favorecido un modelo autoregulatorio (llamado modelo “estadounidense”), encontrándose en medio los que han centrado sus esfuerzos en consolidar mecanismos procesales de protección de la intimidad, generalmente conocidos como “habeas data” (modelo latinoamericano).

La realidad actual, sin embargo, apunta hacia un acercamiento de los diversos sistemas de reconocimiento de la autodeterminación informativa. Los países europeos han permitido la coexistencia de mecanismos de autoregulación en los ficheros de datos personales (códigos de conducta, códigos deontológicos, etc.). Las empresas estadounidenses asimilan estándares cada vez más rigurosos de protección, basándose en muchos casos en las reglas de los países europeos. Finalmente, ante la obsolescencia del habeas data como mecanismo para la tutela de la intimidad, las naciones latinoamericanas se encuentran en un acelerado proceso de actualización de sus marcos regulatorios, acercándolos cada vez más al modelo europeo.

Lo anterior tiene su fundamento quizás en la necesidad asegurar *efectivamente el derecho a la autodeterminación informativa* antes que a defender a ultranza determinados modelos teóricos. Es revelador que el Primer Reporte de Implementación de la Directiva 95/46/CE de la Unión Euro-

[†] Ponencia presentada en el VI Congreso Mundial de Derecho Constitucional, del 12 al 16 de enero de 2004 en Santiago de Chile.

^{**} Licenciado en Derecho por la Universidad de Costa Rica. Doctor en Derecho Constitucional por la Universidade de São Paulo, Brasil. Letrado de la Sala Constitucional de Costa Rica. Profesor de Derecho Constitucional de la Universidad de Costa Rica y de la Universidad Estatal a Distancia.

pea, elaborado por el Grupo de Seguimiento de la Comisión Europea el 15 de mayo de 2003, revela que aún en Europa, donde encuentran los países con estándares más rigurosos y sofisticados de protección de la intimidad, el 81% de las personas estima que el grado de tutela de dicho derecho es insuficiente.¹

Precisamente dentro de este contexto, Costa Rica ha iniciado un lento pero sostenido proceso de modernización de su regulación referente a la protección de las personas frente al tratamiento de sus datos personales. En un primer momento, la jurisprudencia de la Sala Constitucional sentó las bases para un desarrollo legislativo ambicioso, el cual si bien no se ha dado, sí ha originado la presentación de varios proyectos, alguno de los cuales podría llegar a convertirse en Ley de la República y así permitir un adecuado control de la recolección, almacenamiento y manipulación de los datos personales de sus habitantes.

Este breve ensayo pretende describir el proceso que ha seguido Costa Rica en pos de un adecuado nivel de protección de los datos personales, compararlo con el que han experimentado otras naciones de la región, y analizar críticamente la efectividad y viabilidad de las propuestas actuales.

I. DERECHO CONSTITUCIONAL A LA INTIMIDAD

Siguiendo la tradición liberal de su predecesora de 1871, la Constitución Política de 1949 en su artículo 24, *reconoce el derecho a la intimidad en una acepción clásica, protegiendo a la persona frente a la violación de su correspondencia y comunicaciones privadas*. En ese mismo sentido, el numeral 23 de la Constitución reconoce el derecho al domicilio y a la preservación del mismo frente a las intromisiones que pueda sufrir. En ambos casos, se limita severamente la posibilidad de interceptar las comunicaciones o ingresar al domicilio de las personas por parte de los órganos del Estado, en especial de las autoridades jurisdiccionales, y tan sólo en situaciones de verdadera necesidad.

No obstante, este modelo tradicional de protección resulta insuficiente para tutelar el respeto de la persona en lo atinente a su información, en la sociedad altamente tecnificada en que vivimos. La protección contra las interceptaciones telefónicas (o de correo electrónico o correo de voz hoy en día), así como las reglas sobre allanamiento judicial apenas logran cubrir una parte significativa pero incompleta del fuero privado de las personas.

En la era de la información, cada vez que una persona emplea una tarjeta magnética (de uso prácticamente ineludible hoy en día), entra a una página de Internet, ordena una pizza a domicilio, va al médico, etc., deja una huella indeleble que, con la tecnología y la interconectividad suficientes, puede servir para crear del individuo un perfil que lo describa en sus más íntimas preferencias, y que puede servir para los más diversos propósitos.

Las normas de origen liberal que garantizan la intimidad suelen, incluso, estar dirigidas al Estado y otras agencias públicas, cuando en realidad son las grandes corporaciones las que en forma cada vez más acelerada, van adquiriendo la capacidad tecnológica necesaria para irrumpir en el ámbito de intimidad de las personas, llenando sus bases de datos con informaciones diversas acerca de los gustos, costumbres y características de las personas que considera como sus consumidores actuales o potenciales.² Se parte de la premisa de que, sabiendo de antemano las preferencias de su clientela, las empresas podrán ofrecer bienes y servicios cada vez mejores y a menores costos, debido

¹ COMMISSION OF THE EUROPEAN COMMUNITIES. *First report on the implementation of the Data Protection Directive (95/46/EC)*. Brussels: 2003. P. 10.

a la reducción del riesgo.

Ante la necesidad de contener el ímpetu invasor de las empresas administradoras de ficheros, así como de regular el funcionamiento de todas aquellas entidades públicas y privadas encargadas de manipular datos de las personas, la doctrina clásica del derecho a la intimidad y al domicilio requiere evolucionar a una protección integral de la información en todas sus etapas: formación, acopio, almacenamiento y manipulación.

II. DESARROLLO JURISPRUDENCIAL DEL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA

Frente a la escasa regulación existente en Costa Rica, *ha sido la jurisprudencia de la Sala Constitucional de la Corte Suprema de Justicia, al conocer de recursos de amparo*, la que ha ido ampliando el concepto clásico de intimidad, extrayendo de éste un derecho no solo a la privacidad en las comunicaciones, sino incluso imponiendo la preservación de los datos sensibles y delineando las reglas básicas para la recolección, almacenamiento y empleo de informaciones personales no pertenecientes al fuero íntimo del individuo.³

Dos razones fundamentales explican que la necesidad de tutela efectiva del derecho a la autodeterminación informativa de las personas las haya llevado a recurrir mayoritariamente a la vía del amparo constitucional, y menos a otras instancias administrativas y jurisdiccionales. La primera se basa en la ya mencionada carencia de un adecuado marco normativo, lo que genera una frecuente reiteración de infracciones a ese derecho fundamental por parte del Estado y de sujetos privados. En segundo lugar, este fenómeno se explica por la aceptación popular del recurso de amparo como mecanismo más efectivo para la defensa de los derechos de las personas.

La acción de amparo (llamada por la Constitución Política con el poco afortunado nombre de “recurso”) es un proceso jurisdiccional previsto para la defensa de los derechos fundamentales contenidos en la Ley Mayor, así como los provenientes del Derecho Internacional de los Derechos Humanos contra actos (u omisiones) cometidos por autoridades públicas o por particulares en ejercicio de funciones públicas o situados en posiciones jurídicas o fácticas de poder, frente a los cuales los remedios ordinarios resulten tardíos o insuficientes. La Sala Constitucional tiene en forma concentrada la competencia para conocer de los amparos, que pueden ser interpuestos por cualquier persona a favor de sí misma o de un tercero 24 horas al día, los 365 días del año. No se requieren para la presentación del recurso más requisitos que un documento escrito donde se consignen con meridiana claridad los datos de identificación del actor y el amparado, el acto impugnado y la autoridad responsable por el mismo. La sentencia del recurso es obligatoria con efectos *erga omnes*, e implica –en caso de ser acogida la pretensión– la responsabilidad del accionado por los daños y perjuicios ocasionados con el acto impugnado.⁴

La carencia de formalismos propios de otras instancias jurisdiccionales, así como la competencia en manos de un órgano de máximo rango del Poder Judicial y la celeridad con que la Sala

² No obstante sean las empresas privadas las grandes villanas del derecho a la autodeterminación informativa, los acontecimientos recientes (posteriores al 11 de setiembre de 2.001) han demostrado que los Estados, en su lucha desesperada por librarse de la amenaza terrorista, también llegan a convertirse en flagrantes violadores del ámbito de intimidad de sus habitantes, con gravísimas consecuencias en campos tales como el derecho a la no discriminación, a la autodeterminación, etc.

³ CARVAJAL PÉREZ, Marvin. *La protección de los datos personales en Costa Rica*. En *Hermenéutica*. Número 11, agosto de 2002. P. 11.

⁴ *Ibid.* P. 12.

resuelve sus asuntos comparada con la jurisdicción común⁵, han hecho que las personas empleen cada vez más este mecanismo procesal, con un crecimiento sostenido a lo largo de los poco más de trece años de existencia del Tribunal Constitucional.⁶

Conociendo de recursos de amparo tendientes a la tutela de los datos personales, la Sala Constitucional en un comienzo declaró la *confidencialidad de los registros en los archivos criminales, restringiendo su uso apenas a las autoridades policiales y al sujeto registrado*⁷, y determinando la destrucción de la ficha en caso de que se vieran desvirtuados los indicios que tuvieron a dicha persona como sospechosa de haber delinquido.⁸ Asimismo, impuso plazos para la efectivación del llamado “derecho al olvido”, entendiendo que ciertas informaciones podían permanecer en este tipo de bases de datos apenas por un determinado período, facilitando la persecución de delitos pero sin obligar a la persona a tolerar la eterna carga de haber sido indiciado y reseñado.⁹

En diversas ocasiones se ha pronunciado la Sala respecto de la confidencialidad de los datos que, aun formando parte de un expediente de contratación administrativa (que por imperativo democrático debe estar sujeto al más estricto control público y ciudadano), contienen informaciones referentes al giro y situación comercial de las empresas oferentes, cuya divulgación podría poner a la afectada en una situación de vulnerabilidad frente a sus competidores, los cuales podrían acceder a datos altamente sensibles, tales como listas de clientes o proveedores, estados financieros, costos de operación, fórmulas y protocolos de funcionamiento, distorsionando el sistema de libre competencia empresarial.¹⁰

Por el contrario, cuando en expedientes públicos consten informaciones o documentos que no sean confidenciales (íntimos), hayan sido formalmente declarados secretos de Estado, o exista un marcado interés general en su preservación, declarado en acto administrativo motivado¹¹ debe, de conformidad con los términos del artículo 30 de la Constitución, garantizarse su pleno e irrestricto acceso, sin que quepa a la Administración la posibilidad de excusarse en razones de mera conveniencia a fin de impedir que las personas accedan a dicha información.¹²

En los últimos años, sin embargo, la Sala Constitucional superó el umbral de protección de los datos íntimos, desarrollando en forma paulatina una extensa doctrina en materia de protección de los datos personales desde una perspectiva mucho más amplia. Si bien la jurisprudencia constitucional no ha seguido un camino constante en esta dirección¹³, lo cierto es que una serie de fallos enfocados en la misma dirección ha ido delineando los aspectos fundamentales de la protección de datos personales.

Por un lado, las sentencias números 4154-97, 7175-97, 4347-99 y 5802-99 reconocieron la existencia de un derecho a la tutela jurisdiccional privilegiada de los datos personales (hábeas data), desarrollando una serie de principios atinentes al acopio, almacenamiento y empleo de bases de datos, lista que ha sido ampliada y delimitada por diversos fallos posteriores, tales como las senten-

⁵ En 2.002, la duración promedio de un recurso de amparo era de once semanas desde su presentación hasta el dictado de la sentencia. La duración promedio de un proceso contencioso administrativo oscilaba al rededor los treinta meses solo para la obtención de una sentencia de primer instancia. Fuente: Departamento de Estadística del Poder Judicial.

⁶ En 2.002, la Sala Constitucional conoció cerca de 11.500 recursos de amparo, para un total cercano a los 13.500 asuntos conocidos en el año. Fuente: Secretaría Administrativa de la Sala Constitucional.

⁷ Cfr. sentencias números 2609-91, 2680-94 y 2256-95.

⁸ Cfr. sentencias 476-91 y 9640-02.

⁹ Cfr. sentencias 2805-98, 8218-98 y 5802-99.

¹⁰ Cfr. sentencia 6481-99.

¹¹ Cfr. sentencia 7265-99.

¹² Cfr. sentencias 3074-02 y 3489-03.

¹³ La sentencia número 2563-99, por ejemplo, casi desconoce la existencia del derecho y la posibilidad de su tutela por vía de amparo.

cias números 1345-98, 1119-00 y 00754-02, que reconocen expresamente la existencia de un derecho a la autodeterminación informativa y desarrollan en detalle sus postulados esenciales, en particular el principio de calidad de los datos y de adecuación al fin para el cual fueron obtenidos. Estas tres sentencias demuestran que la Sala Constitucional decidió entender en forma amplia la relación existente entre el derecho a la intimidad y el principio democrático, observándola como un presupuesto esencial para el ejercicio de otros derechos fundamentales previstos en la Constitución, 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.¹⁴

Finalmente, la sentencia número 08996-02 va todavía más allá y reconoce los derechos a recibir información acerca del uso que será dado a los datos suministrados, al consentimiento necesario para que tales informaciones puedan ser recogidas, almacenadas y manipuladas, y sienta algunas bases de lo que deberá en el futuro ser la regulación de la transferencia nacional e internacional de datos entre diversos ficheros. Es decir, recoge muchos de los principios modernamente entendidos como propios de una adecuada protección de datos.

Así, el desarrollo de la jurisprudencia constitucional en torno al derecho a la autodeterminación informativa podría ser resumida en los siguientes puntos esenciales:

- Cabe el recurso de amparo tanto para la protección de los datos personales contenidos en bases de datos públicas como para los almacenados en archivos privados. Las agencias particulares que almacenan este tipo de datos (empresas protectoras de crédito, por ejemplo) pueden ser accionadas por entenderse que se encuentran, respecto del particular, en una situación fáctica de poder, debido a la enorme cantidad y calidad de datos que pueden almacenar en medios cada vez más eficientes y difíciles de rastrear (artículo 57 de la Ley de la Jurisdicción Constitucional).
- Los datos pertenecientes al fuero interno de la persona, conocidos generalmente como “datos sensibles”, referidos a los aspectos propios de su individualidad (preferencias sexuales, ideología, creencias religiosas, etc.) no pueden del todo ser recolectados sin el expreso consentimiento del titular. Mucho menos almacenados y difundidos.
- Respecto de los otros tipos de datos que aunque referidos a particulares tienen una finalidad pública (informaciones contenidas en los archivos médicos, policiales, judiciales, etc.), su acceso se encuentra restringido a los órganos de la Administración Pública directamente autorizados, así como a los propios dueños de los datos.
- Los datos estrictamente públicos contenidos en bases de datos, igualmente públicas, pueden ser accedidos por cualquier persona que así lo solicite, siempre que no se trate de secretos de Estado u otras situaciones calificadas –descritas en acto motivado– en que la revelación de los datos podría afectar gravemente el interés general.¹⁵
- Informaciones referentes al historial bancario y crediticio de la persona son de acceso restringido. Sin embargo, el incumplimiento de obligaciones reviste interés supraindividual, con la finalidad de mantener el clima de confianza necesario en el mercado financiero, y evitar así el aumento del riesgo y sus efectos en la fijación de las tasas de interés. Tampoco protege el secreto

¹⁴ CARVAJAL PÉREZ, Marvin y CHIRINO SÁNCHEZ, Alfredo, *El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica*. En *Revista de Derecho Constitucional*. San José: Instituto Costarricense de Derecho Constitucional. Número 4. 2003. P. 251.

¹⁵ Tal fue el caso conocido por la Sala al dictar la sentencia 07265-99, rechazando la solicitud de un periodista para que se ordenara al Ministerio de Seguridad Pública publicar el contenido de un informe elaborado por la DEA y que contenía datos relativos a las rutas de entrada y salida de las drogas en el país, que luego serían usadas en el combate contra el narcotráfico.

bancario las cuentas de los partidos políticos o las que hayan sido empleadas para recibir fondos para una campaña electoral.¹⁶

- Los bancos de datos, públicos y privados, deben regirse por las siguientes reglas: transparencia sobre el tipo, dimensión o fines del procesamiento de los datos guardados; correspondencia entre los fines y el uso y almacenamiento de la información; exactitud, veracidad, actualidad y plena identificación de los datos guardados; libre acceso por parte de los interesados y posibilidad de exigir la rectificación de los mismos, si bien dicha petición no constituye un requisito previo a la interposición del recurso de amparo.
- La necesidad de un organismo de control que vele porque el tratamiento automatizado de datos cumpla los principios que protegen el derecho de los ciudadanos a su autodeterminación informativa.
- El derecho al olvido: los datos no pueden mantenerse indefinidamente en un banco de datos, transcurrido el plazo establecido o razonable, deben ser destruidos.

A partir de las reglas reconocidas por la Sala Constitucional en relación con los datos personales, en razón de la eficacia general que tienen su jurisprudencia y sus precedentes, de conformidad con el artículo 13 de la Ley de la Jurisdicción Constitucional, el ciudadano que se vea afectado en su derecho a la autodeterminación informativa por violación a cualquiera de los principios enumerados, puede acudir a la vía del amparo constitucional y reclamar allí la exclusión o corrección de los datos respectivos. De obtener una sentencia estimatoria, la Sala ha optado por dar un plazo a la agencia pública o privada para que cumpla con la orden respectiva, so pena de incurrir en el delito de desobediencia a la autoridad.¹⁷

III. PROPUESTA DE CREACIÓN DE UN REMEDIO CONSTITUCIONAL ESPECÍFICO: EL "HABEAS DATA"

Desde inicios de la década de 90, en Costa Rica se comenzó a discutir acerca de la necesidad de establecer un marco jurídico adecuado para la protección de los datos personales.¹⁸ Es así como en 1.996, un proyecto de ley intentó introducir una reforma a la vigente Ley de la Jurisdicción Constitucional, a fin de que se adicionara un Capítulo IV referido al "Hábeas Data" en el Título III sobre los recursos, como una forma de "amparo específico" en materia de tutela de la "identidad" o "libertad" informáticas.¹⁹

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

¹⁶ La sentencia número 3489-03 negó el carácter de confidenciales a los estados bancarios y desgloses de operaciones referentes a las cuentas del Partido Unidad Social Cristiana y de algunas sociedades anónimas que se acusa de haber recibido fondos destinados a financiar la campaña electoral de dicha agrupación.

¹⁷ Carvajal Pérez, Marvin. *La protección de los datos personales en Costa Rica*. En *Hermenéutica*. Número 11, agosto de 2002, p. 12.

¹⁸ El tratadista nacional Alfredo Chirino, en varios de sus escritos, llamó la atención acerca de los riesgos que en el ámbito de intimidad produce el acelerado progreso de las tecnologías de la información. Cfr. CHIRINO SÁNCHEZ, Alfredo, *Informática y Derecho a la intimidad. Perspectivas de política criminal*. San José: CONAMAJ, 1991. Y *Autodeterminación informativa y Estado de Derecho en la sociedad tecnológica*. San José, CONAMAJ, 1997.

¹⁹ Expediente legislativo número 12.827, que fue archivado en 1.988 y presentado de nuevo en 2.002 con los números 14.778 y 14.785.

El así llamado “hábeas data 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 recolección y grabación de los datos o, por ejemplo, la transmisión de datos más allá de las fronteras.²⁰

El proyecto contemplaba la creación de una garantía jurisdiccional específica, destinada a proteger los derechos a la autodeterminación informativa, la intimidad y la libertad informática. La solución propuesta, sin embargo, pecaba de insuficiente, pues planteada apenas la existencia de un remedio reaccional o represivo, que entraría a regir una vez que la violación a los derechos del interesado ya hubiera ocurrido. También se caía en el error de sacar los derechos que se pretendía tutelar del ámbito protector de la acción (genérica) de amparo, para que fueran garantizados por un proceso mucho más formalista y menos accesible que el ordinario. Con la buena intención de reforzar la tutela del derecho a la intimidad, se dificultaba el ejercicio de su efectiva protección.

Otro aspecto que lleva a entender como insuficiente el proyecto en comentario es el que en éste haya sido asignada la protección del derecho a la autodeterminación informativa al tribunal constitucional no especializado en materia tan específica y técnica como la manipulación de bases de datos, la transmisión de información, etc. En todo caso, la Sala Constitucional ya venía conociendo de recursos de amparo en esta materia, por lo que la aprobación del proyecto en cuestión implicaba una innovación muy limitada.

Junto con los anteriores razonamientos, no puede dejar de ser considerado que la mayoría de los países latinoamericanos que adoptaron en sus ordenamientos constitucionales y legales la figura del habeas data lo hizo como respuesta a la invasión del ámbito privado llevada a cabo por el Estado durante el auge de la teoría de la seguridad nacional, que sostuvo ideológicamente diversas prácticas represivas por parte de los regímenes autoritarios que asolaron nuestra región especialmente durante las décadas de 1960 y 1970. No se trata, pues, de un remedio concebido para la defensa contra la manipulación de datos que realizan las corporaciones mercantiles, asociaciones civiles, partidos políticos, etc.

Además, en la casi totalidad de países donde fue incluido como remedio procesal, el habeas data no ha dado los resultados esperados o simplemente es insuficiente ante las nuevas realidades, y de hecho la mayoría de los Estados latinoamericanos han iniciado un proceso de adecuación de sus normas sustantivas a las nuevas exigencias del derecho a la autodeterminación informativa, y asimismo se plantean la necesidad de crear instancias administrativas de control del manejo de los datos personales.

IV. PROYECTO DE LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES

Como respuesta a la carencia de regulación adecuada y específica para la protección de los datos de las personas en Costa Rica, y ante la necesidad de implementar un marco normativo que permita una tutela preventiva de la intimidad, así como los mecanismos procedimentales necesarios para reaccionar con efectividad ante la violación de tales derechos fundamentales, un grupo de catorce

²⁰ CARVAJAL PÉREZ, Marvin y CHIRINO SÁNCHEZ, Alfredo, *El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica*. En *Revista de Derecho Constitucional*. San José: Instituto Costarricense de Derecho Constitucional. Número 4. 2003. P. 235.

diputados pertenecientes a cuatro distintas fracciones legislativas presentó un proyecto de ley que recoge buena parte de la experiencia comparada en esta materia, así como la evolución de la jurisprudencia constitucional. A esta iniciativa, denominada proyecto de “Ley de protección de la persona frente al tratamiento de sus datos personales” o “Ley PRODAT”²¹ le fue asignado el número de expediente 15.178.

El primer aspecto que cabría preguntarse es si una iniciativa de esta naturaleza puede ser aprobada por el legislador ordinario, o si, por el contrario, requeriría de una reforma parcial a la Constitución Política, a fin de que allí sea reconocido expresamente el derecho de los individuos a que se haga buen uso de sus datos personales. Al respecto, debe concluirse, necesariamente, que la jurisprudencia constitucional reconoció la existencia del derecho a la autodeterminación informativa, a partir de una interpretación extensiva del artículo 24 constitucional. Es obvio, por ende, que resulta innecesaria la reforma a la Constitución, pues la misma (una norma no escrita de ésta, como es la jurisprudencia constitucional) ya contiene la previsión respectiva, por lo que corresponde al legislador ordinario su debido desarrollo. De hecho, dado el carácter fundamental que la Sala Constitucional ha reconocido a la autodeterminación informativa, cabría preguntarse si –por el contrario– la ausencia de una adecuada regulación legal que garantice el respeto del mencionado derecho no configura una omisión inconstitucional.²²

El proyecto tiene como objetivo garantizar a cualquier persona física o jurídica, sea cual fuere su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida privada y demás derechos de la personalidad; asimismo, la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes. Como se ve, la finalidad del mismo es desarrollar tanto una regulación de carácter preventivo, así como la inclusión de mecanismos para lograr una eficaz reacción frente a los riesgos que pueda sufrir el derecho a la autodeterminación informativa. También, cabe destacar que no hace distinción entre el tipo de sujetos protegidos, lo que permite una protección sumamente amplia y adaptable de ese derecho.²³

Para lograr sus objetivos, el proyecto consagra el derecho de información que sobre los ficheros tienen las personas, determinando la necesidad de que, al momento de serles requerida una información, se les informe claramente la existencia de la base de datos, de la finalidad de la recolección y los destinatarios de la información, de la posibilidad de ejercer los derechos de acceso, rectificación, actualización, cancelación y confidencialidad; y de la identidad y dirección del responsable del fichero. Como derivación de lo anterior, se prevé que el titular de los datos dé por sí o por su representante, el consentimiento para la entrega de los datos, salvo que la ley disponga otra cosa dentro de límites razonables.

Establece reglas referentes a la calidad de los datos personales, imponiendo que solo podrán ser recolectados, almacenados y empleados datos de carácter personal para su tratamiento automatizado o manual, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades legítimas para las que hayan sido obtenidos. No podrán ser utilizados para propósitos distintos de aquellos que motivaron su recolección. Deberán ser exactos y actuales, de forma que respondan con veracidad a la situación real del afectado.

El proyecto también determina un régimen reforzado de protección para los llamados datos sensibles: informaciones de carácter personal de las personas físicas que revelen su origen étnico,

²¹ En alusión al órgano administrativo que crea y al que encarga la protección preventiva y represiva de los datos personales.

²² CARVAJAL PÉREZ, Marvin y CHIRINO SÁNCHEZ, Alfredo, *El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica*. En *Revista de Derecho Constitucional*. San José: Instituto Costarricense de Derecho Constitucional. Número 4. 2003. P. 265.

²³ *Ibid.* P. 266.

opiniones políticas, convicciones religiosas o espirituales, así como los datos de carácter personal relativos a la salud, a la vida sexual y a sus antecedentes delictivos. Este tipo de datos no podrá ser almacenado de manera automática ni manual en registros o ficheros privados, y en los registros públicos su acceso será restringido. Se busca, claramente, proteger en estos casos el fuero íntimo de la persona, aquellos aspectos que revelan los rasgos más característicos de su personalidad, con el objeto de evitar exponer su intimidad al conocimiento público o de hacer uso de dicho conocimiento para cualquier motivo ajeno a la voluntad del titular.²⁴

Establece los principios que deben seguir los responsables de los ficheros, a efecto de garantizar la seguridad de los datos almacenados y evitar así su alteración, pérdida, tratamiento o acceso no autorizado. Prohíbe expresamente el registro de datos en ficheros automatizados que no reúnan las condiciones de garantía plena de seguridad e integridad. El responsable del fichero y quienes intervengan en cualquier fase del proceso de recolección y tratamiento de los datos de carácter personal, están obligados a guardar el secreto profesional.

Dispone que la cesión de los datos contenidos en los ficheros, solo resulta procedente para fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento del afectado, sin importar si se trata de ficheros públicos o privados. Se pretende evitar que la cesión de datos provoque un incumplimiento fraudulento a las diversas reglas de fondo previstas.

A la persona se le garantiza el derecho a conocer de la existencia del fichero y sus finalidades principales, así como la identidad y domicilio del encargado del mismo; a obtener, con intervalos razonables y sin demora, la confirmación de la existencia de sus datos en archivos o bases de datos; a obtener, si procediere, la rectificación de dichos datos, su actualización o la eliminación de los mismos.

Toda persona debe además contar con un recurso administrativo sencillo y rápido ante la Agencia de Protección de Datos (órgano creado por la misma ley), con el fin de ser amparada contra actos que violen su derecho a la autodeterminación informativa, sin perjuicio de los mecanismos procesales que la ley establezca para este mismo fin. La anterior previsión, además de establecer un mecanismo de control administrativo de los archivos y bases de datos, deja a salvo la posibilidad de que el buen uso de los datos personales siga siendo tutelado por la vía del amparo especial que, como se dijo supra, ha desarrollado la jurisprudencia constitucional. Tal coexistencia de mecanismos administrativos y jurisdiccionales para la defensa de determinados derechos fundamentales no es novedosa en nuestro ordenamiento, tal es el caso, entre otros, de la tutela del medio ambiente, del derecho a la libre competencia, de los derechos del consumidor, de la protección de los menores de edad, etc.

Prevé la posibilidad de que las personas y agencias, públicas o privadas, encargadas de ficheros, puedan emitir protocolos de actuación, inscritos ante el Registro de Archivos y Bases de Datos, órgano de la PRODAT. La manipulación de datos con base en un protocolo de actuación inscrito ante la Agencia hará presumir (*iuris tantum*) el cumplimiento de las disposiciones contenidas en la ley, para los efectos de autorizar la cesión de datos contenidos en un archivo o base. Resulta interesante apreciar cómo en la iniciativa de comentario se estaría combinando el uso de mecanismos de regulación (sistema europeo) y de autorregulación (sistema estadounidense), tal como pareciera ser el signo de los tiempos actuales, en que las naciones europeas, cada vez más, ven como sus empresas suscriben códigos de conducta que hacen más ágil la transmisión y uso de datos, mientras que las agencias estadounidenses desarrollan sus protocolos de actuación de manera que reflejan más y más las reglas que contienen las modernas y detalladas normas de los países europeos²⁵.

²⁴ Op. Cit. P. 268.

Prohíbe la transferencia internacional de datos personales, excepto los casos que la PRODAT autorice, por corroborar que con dicho traslado no están siendo vulnerados los principios rectores del manejo de datos personales, y si el receptor está domiciliado o tiene como base un país que ofrezca un nivel de protección de los datos personales igual o superior al establecido en Costa Rica. Esta regla es una de las más ambiciosas prevista en el anteproyecto, pues pretende prevenir la violación de las reglas sobre manejo de datos personales producto de la indebida cesión a personas domiciliadas en países que cuentan con una pobre protección de datos personales (“paraísos” del trasiego y manejo de datos). Con ello, Costa Rica estaría regulando la materia en forma similar a la prevista en la normativa desarrollada por la Unión Europea²⁶, que de manera expresa proscribió la transmisión de datos hacia sitios “poco seguros”.²⁷

Para el control de todas aquellas personas, empresas e instituciones encargadas del manejo de archivos y bases de datos personales, el proyecto 15.178 prevé la creación de un órgano dotado de independencia funcional y de criterio, adscrito a la Asamblea Legislativa, denominado Agencia para la Protección de Datos Personales (PRODAT). Se ha buscado diseñar un órgano de carácter eminentemente técnico y dotado con los medios necesarios para la efectiva garantía de los derechos derivados del manejo de datos personales, con lo que se rompe la tradición latinoamericana (con las excepciones ya mencionadas) de asignar a los órganos jurisdiccionales el conocimiento de los procesos de hábeas data.

Dicha institución tendría entre sus funciones velar por el cumplimiento de la normativa en materia de protección de datos; llevar un registro de los archivos y bases de datos que sean propiedad o estén en administración tanto de personas físicas como de entes y órganos públicos y privados; requerir, de quienes posean o administren archivos y bases de datos, las informaciones necesarias para el ejercicio de su cargo, pudiendo incluso acceder a sus registros, con el fin de hacer cumplir efectivamente las normas sobre protección de datos personales; autorizar la transferencia de datos entre diversos ficheros; atender los reclamos por infracción a las normas sobre protección de datos personales; ordenar, de oficio o a petición de parte, la supresión, rectificación, adición o restricción en la circulación de las informaciones contenidas en archivos y bases de datos, cuando contravengan las normas sobre protección de datos personales; imponer las sanciones administrativas establecidas en la ley a quienes infrinjan las normas sobre protección de datos personales, y fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, almacenamiento, transferencia y uso de sus datos personales.

La Dirección de la PRODAT recae sobre un director o directora nacional designado (a) por la Asamblea Legislativa. Permanecerá en su cargo durante seis años, con posibilidad de reelección hasta por una vez. Durante su gestión no podrá ser removido sino por justa causa, con garantía del debido proceso, por el voto de la mayoría absoluta de los diputados presentes en el plenario legislativo.

Dispone que la Agencia contará con el personal técnico y administrativo necesario para el buen ejercicio de sus funciones, designado mediante concurso por idoneidad. Le ordena además capacitar permanentemente a su personal en el manejo de nuevas herramientas tecnológicas y nuevas formas de manejo de datos personales. Prohíbe a todos los empleados de la PRODAT prestar servicios a las

²⁵ Gellman, Robert. *Privacy Benefits and Costs From US Perspective* y Buttarelli, Geovanni. *Diritti fondamentali e libertà d'iniziativa economica*. Ponencias presentadas en el seminario *Privacy: da costo a ricorsa*. Roma, diciembre de 2002.

²⁶ Convención de Estrasburgo de 28 de enero de 1981, Directiva 95/46 del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 y Directiva 97/66 del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997.

²⁷ CARVAJAL PÉREZ, Marvin y CHIRINO SÁNCHEZ, Alfredo, *El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica*. En *Revista de Derecho Constitucional*. San José: Instituto Costarricense de Derecho Constitucional. Número 4. 2003. P. 272.

personas o empresas que se dediquen al acopio, almacenamiento o manejo de datos personales, hasta dos años después de haber cesado en sus funciones; revelar los datos a que ha tenido acceso con ocasión de su cargo, en cualquier tiempo, aun después de haber cesado en el cargo.

El proyecto determina la organización básica de la Agencia: el director o directora nacional, el subdirector o subdirectora nacional, el Registro de Archivos y Bases de Datos, el Departamento de Inspección de Archivos y Bases de Datos, y el Departamento de Divulgación, al que corresponde la elaboración y ejecución de una estrategia de comunicación dirigida a permitir que los habitantes conozcan los derechos derivados del manejo de sus datos personales, así como los mecanismos que el ordenamiento prevé para la defensa de tales prerrogativas.

Prevé la posibilidad de que cualquier persona que ostente un derecho subjetivo o un interés legítimo, denuncie ante la PRODAT que un archivo o base de datos, público o privado, actúa en contravención de las reglas para el manejo de datos personales. Recibida la denuncia, el Departamento de Inspección conferirá al encargado del fichero un plazo de tres días hábiles para que informe, disponiendo que si se tratare de una autoridad pública el informe será tenido bajo juramento. La omisión de rendir el informe en el plazo estipulado hará que se tengan por ciertos los hechos acusados. En cualquier momento, el Departamento de Inspección podrá ordenar al denunciado la presentación de la información necesaria, o efectuar inspecciones *in situ* en sus ficheros. A más tardar un mes después de la presentación de la denuncia, el Departamento de Inspección debe presentar al director o directora nacional una recomendación respecto de la procedencia de la denuncia. Transcurridos cinco días el director o directora nacional deberá dictar el acto final. Contra su decisión cabrá recurso de reconsideración dentro del tercer día, el cual deberá ser resuelto en el plazo de ocho días luego de recibido, agotando la vía administrativa.

Si el director o directora nacional determinare que la información del afectado es falsa, incompleta, inexacta, o bien que la misma fue indebidamente recolectada, almacenada o difundida, deberá ordenar su inmediata supresión, rectificación, adición o aclaración, o bien impondrá una restricción respecto de su transferencia y difusión, conminándolo a sufrir las penalidades previstas en ésta y otras leyes en caso de incumplimiento.

De oficio o a instancia de parte, podrá el PRODAT iniciar procedimiento tendiente a demostrar si un archivo o base de datos está siendo empleado de conformidad con sus principios. El proyecto prevé sanciones administrativas que podrían ser aplicadas a los ficheros: para las faltas leves, multa de hasta cinco salarios base; para las faltas graves, multa de hasta diez salarios base y suspensión para el funcionamiento del fichero de uno a seis meses; para las faltas gravísimas, multa de hasta veinte salarios base y suspensión para el funcionamiento del fichero de uno a cinco años.

El régimen sancionatorio previsto en el proyecto no excluye la posibilidad de que la comisión de alguna de las faltas tipificadas por parte de los encargados de ficheros, así como de los funcionarios de la PRODAT, pueda acarrear responsabilidades de otros géneros, como la penal o la indemnizatoria. De lo contrario, podría haber sido dejada sin contenido, para estos efectos, la norma contenida en el artículo 41 de la Constitución Política. No cabe duda, sin embargo, que el uso de mecanismos sancionatorios administrativos permite una mayor flexibilidad que la dada por las sanciones penales, como por ejemplo en la posibilidad de sancionar personas jurídicas mediante procedimientos y reglas que, si bien deben respetar el debido proceso, no estén sometidas a la ritualidad propia del ejercicio del sistema de justicia penal.²⁸

²⁸ Op. Cit. P. 282.

V. ALCANZAR UN NIVEL ADECUADO DE PROTECCIÓN COMO META

Es claro que la misma naturaleza del derecho fundamental en juego, así como su incidencia en el ejercicio y disfrute pleno de otros derechos y valores constitucionales, tales como la libertad personal, el honor, la autodeterminación de los individuos, la seguridad personal y patrimonial, e incluso el mismo sistema democrático. No obstante, a las anteriores razones –suficientes de por sí para legitimar un esfuerzo de actualización normativa e implementación eficaz– se deben sumar otras de carácter económico y político que refuerzan la necesidad de una actuación inmediata y decidida.

Por un lado, diversos acontecimientos han incrementado el grado de atención que la opinión pública y los grupos de poder vienen dando al problema.²⁹ Asimismo, varias instituciones públicas, tales como el Ministerio de Justicia y Gracia y la Defensoría de los Habitantes de la República se pronunciaron recientemente acerca de la necesidad de implementar a la brevedad, mecanismos efectivos de control acerca del manejo de datos personales en el país.³⁰

En la XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, efectuada en Santa Cruz de la Sierra, Bolivia en noviembre de 2.003, los representantes de los Estados suscribieron la llamada “Declaración de Santa Cruz de la Sierra”, que en su artículo 45 reconoce que la protección de los datos personales es un derecho fundamental de las personas, y destaca la importancia de las iniciativas regulatorias contenidas en la Declaración de La Antigua, Guatemala por la que se crea la Red Iberoamericana de Protección de Datos.³¹ Igualmente, las llamadas “Reglas de Heredia” o “Reglas mínimas para la difusión de información judicial en Internet”³² reconocen que el deber de transparencia de las dependencias estatales –incluida la Justicia– no se impone a la necesidad de preservar la intimidad de los usuarios del sistema judicial, sino que debe ser buscado un sano punto de equilibrio entre ambos valores.

No cabe duda que en momentos en que el país (en conjunto con las otras naciones centroamericanas) se encuentra negociando un tratado de libre comercio con los Estados Unidos y con el posible lanzamiento del ALCA a mediano plazo, la necesidad de establecer un adecuado y moderno estatuto jurídico de la privacidad resulta, a todas luces, indispensable.

En el plano internacional, la necesidad cada vez mayor que tienen los Estados de intensificar sus relaciones de intercambio hace que para los países periféricos resulte de particular relevancia eliminar todas las barreras posibles a la entrada de sus productos en los mercados más fuertes. Así, la emisión de las Directivas 95/46/CE y 97/66/CE de la Unión Europea, y particularmente las disposiciones referente a la transferencia internacional de datos ha llevado a los países latinoamericanos a iniciar una saludable y acelerada carrera por adecuar sus estándares domésticos a las rigurosas reglas europeas.³³

²⁹ Los medios de comunicación dieron especial atención en su momento hechos tales como la aparente interceptación de llamadas telefónicas en la Asamblea Legislativa (La Nación, 11 de mayo de 2.002; La República, 11 de mayo de 2.002); el tráfico de datos por parte de diversas entidades costarricenses y de otros países latinoamericanos a la empresa Choice Point, la que a su vez los vedó a autoridades policiales y migratorias y a empresas privadas estadounidenses (La Nación, 21 de mayo y 5 de junio de 2.003); el allanamiento en Managua, Nicaragua, de las oficinas de una agencia protectora de crédito de capital costarricense por supuesta manipulación indebida de información personal (La Nación, 27 de abril de 2.003); la propuesta de formación del “T.I.A.” (“Terrorism” Information Awareness), mega base de datos que administraría el Departamento de Defensa de los Estados Unidos de América para la prevención de ataques contra su seguridad interna (La Nación, 2 de julio de 2.003); etc.

³⁰ Informe de la Comisión sobre Comercio de Datos Personales, coordinada por la Ministra de Justicia y Gracia, emitido el 3 de setiembre de 2.003, e informe de la Defensoría de los Habitantes de la República de 24 de noviembre de 2.003.

³¹ <http://www.secib.org>

³² http://www.ijjusticia.edu.ar/Reglas_de_Heredia.htm

³³ Argentina promulgó en 2.001 la Ley 25.326 Ley de Protección de Datos Personales, asimismo emitió los Decretos 995/2000 sobre el Régimen Legal del Habeas Data y 1558/2001 que reglamenta la Ley 25.326; Brasil en 1.997 emitió la Ley 9.507 que Regula el derecho de acceso a informaciones y disciplina el procedimiento del habeas data; Chile promulgó la Ley número 19.628 de 1.999, sobre

Como parte de ese esfuerzo modernizador, Argentina logró ser el primer país de la región declarado por la Comisión Europea como Estado que reconoce un adecuado nivel de protección, a los efectos de la Directiva 95/46/CE.³⁴ Lo anterior lo logró merced a una profunda modificación normativa, al promulgar la Ley 25.326, que contempla la creación de un órgano de control fuerte e independiente; toma de previsiones respecto del derecho de información y consentimiento del titular de los datos; del reconocimiento del principio de calidad de la información almacenada y difundida; de su necesaria seguridad; de los derechos de acceso, rectificación y reposición; por haber regulado las transferencias de datos; regular un nivel calificado de protección para los datos sensibles; prever sanciones efectivas y disuasivas; y permitir el empleo del habeas data como remedio ante la violación de tales derechos.

Con el proyecto de Ley PRODAT, Costa Rica pretende alcanzar adecuados estándares de protección de los datos de sus habitantes, y al mismo tiempo evitar que al país se le llegue a considerar un “paraíso” del tráfico de información personal. Para ello, y según ha sido descrito en el aparte anterior, la iniciativa en cuestión contiene todos los elementos que la Comisión Europea ha estimado suficientes para declarar a un país como destino seguro, e incluso podría superar tales requerimientos, dada la pretensión de constituir un órgano altamente independiente—dada su adscripción directa al Parlamento y la independencia funcional y de criterio que se le asegura— así como la disposición de una pluralidad de mecanismos de garantía, permitiendo a las personas defenderse de la vulneración de sus derechos ante la Agencia o ante la Sala Constitucional.

CONCLUSIÓN

La regulación actualmente vigente en Costa Rica no es suficiente para permitir una adecuada tutela de la intimidad de sus habitantes. Los preceptos constitucionales son genéricos y propios de una realidad histórica mucho menos compleja que la actual. El desarrollo explosivo de los medios de almacenamiento, procesamiento y transmisión de datos hace necesaria una intervención estatal cada vez mayor en este campo. Si bien muchos campos de la actuación pública y privada vienen sufriendo un proceso de paulatina desregulación, ese no es el caso del tratamiento de datos personales, que en el estadio actual de evolución requieren de una firme y comprensiva intervención estatal, tendiente a evitar cualesquiera abusos que se intente cometer por parte de las instituciones y empresas encargadas de dicha actividad.

La jurisprudencia de la Sala Constitucional ha venido interpretando en forma sumamente amplia la parca redacción del artículo 24 de la Ley Fundamental, de modo que ha extraído de éste la existencia de un derecho a la autodeterminación informativa, e imponiendo a los operadores de bases de datos mayores restricciones en el ejercicio de su actividad. Dada la amplia accesibilidad e informalidad de la justicia constitucionalidad, así como por la fuerza vinculante de sus decisiones, este desarrollo jurisprudencial ha revestido la mayor importancia. No obstante, los mecanismos procesales de tutela son, la mayoría de las veces, reaccionales y no preventivos, y su importancia se restringe en buena medida al establecimiento de bases generales de actuación y solución de casos concretos.

protección de la vida privada; México aprobó en 2.002 la Ley 19.628, sobre protección de la vida privada. Además, Brasil, Panamá, Nicaragua, Guatemala, Colombia, Costa Rica y Uruguay tienen en diversos grados de avance, proyectos (o anteproyectos) tendientes a modernizar sus marcos regulatorios en materia de protección de datos personales.

³⁴ Cfr. COMISIÓN EUROPEA: GRUPO DE TRABAJO DE PROTECCIÓN A LAS PERSONAS EN LO QUE RESPECTA A DATOS PERSONALES. *Dictamen 4/2002 sobre el nivel de protección de datos personales en Argentina*. 3 de octubre de 2.002.

Así, la implementación de un sistema permanente de control de las bases de datos es tarea del legislador, el cual debe proceder a la brevedad a aprobar un marco regulatorio actual y adecuado, se trate del proyecto de “Ley de protección de la persona frente al tratamiento de sus datos personales” o de cualquier otra iniciativa que discipline la materia en forma moderna y eficaz. Dejando de lado razonamientos contables simplistas, el país debe asumir el reto de diseñar una estructura administrativa independiente y dotada de poderes y herramientas suficientes para garantizar en forma plena la protección de los datos de las personas, sin perjuicio de la función tutelar que ha venido desempeñando hasta ahora la Sala Constitucional.

Los países de la región latinoamericana no pueden seguir siendo regulados por normas obsoletas e insuficientes para la protección del individuo visto como centro de la sociedad y del sistema normativo. Dar el paso hacia la tutela efectiva de la intimidad de las personas es un salto en dirección al respeto integral de su personalidad, de su condición de ser único e irrepetible cuya salvaguarda debe estar por encima de cualesquiera intereses mercantiles y materialistas. La democracia del siglo XXI es el régimen de la transparencia del Estado y las instituciones, pero al mismo tiempo es el del respeto pleno de la persona y de su círculo impenetrable de derechos. Nos corresponde ahora actuar en cumplimiento de este deber histórico.

BIBLIOGRAFÍA:

- BUTTARELLI, Giovanni. *Libertà di iniziativa economica. Privacy, da Costo a Ricorsa*. Roma, 2002.
- CARVAJAL PÉREZ, Marvin. *La protección de los datos personales en Costa Rica*. En *Hermenéutica*. Número 11, agosto de 2002.
- CARVAJAL PÉREZ, Marvin y CHIRINO SÁNCHEZ, Alfredo, *El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica*. En *Revista de Derecho Constitucional*. San José: Instituto Costarricense de Derecho Constitucional. Número 4. 2003.
- CHIRINO SÁNCHEZ, Alfredo, *Autodeterminación informativa y Estado de Derecho en la sociedad tecnológica*, San José, CONAMAJ, 1997, (citado como “Autodeterminación”).
- CHIRINO SÁNCHEZ, Alfredo. “El ‘hábeas data’ como realización del derecho a la autodeterminación informativa. Ideas en torno a un proyecto de ley” in *Revista Parlamentaria*. Vol 5. No. 2. Agosto 1997.
- COMISIÓN EUROPEA: GRUPO DE TRABAJO DE PROTECCIÓN A LAS PERSONAS EN LO QUE RESPECTA A DATOS PERSONALES. *Dictamen 4/2002 sobre el nivel de protección de datos personales en Argentina*. 3 de octubre de 2002.
- ESCOBAR DE LA SERNA, Luis. *Principios del derecho a la información*. Madrid: Dickynson, 2000.
- FERREIRA FILHO, Manoel Gonçalves. *Direitos Humanos Fundamentais*. São Paulo: Saraiva, 2002.
- GELLMAN, Robert. *Privacy Benefits and Costs From a U.S. Perspective*. *Privacy, da Costo a Ricorsa*, Roma, 2002.
- HERNÁNDEZ VALLE, Rubén. *Derecho Procesal Constitucional*. San José: Juricentro, 1994.
- HERRÁN ORTIZ, Ana Isabel, *La violación de la intimidad en la protección de datos personales*, Madrid: Dickynson, 1999.
- MAGLIO, Marco, *Analisi economica del diritto alla riservatezza*. *Privacy, da Costo a Ricorsa*, Roma, 2002.
- MIERELLES, Helly Lopes, *Mandado de segurança. Ação popular. Ação civil pública. Mandado de injunção. “Habeas data”*. São Paulo: Malheiros, 1996.

- MORELLO, Augusto M., *Las garantías jurisdiccionales para la tutela eficaz de los derechos humanos en Iberoamérica*, en *Revista de Processo*. São Paulo. 16(62): 194-204, abril/junho de 1991.
- MURILLO, Pablo Lucas, *El derecho a la autodeterminación informativa*. Madrid: Tecnos, 1990.
- PAISSAN, Mauro. *Quale privacy? Privacy, da Costo a Ricorsa*. Roma, 2002.
- 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.
- QUESADA M., Juan Gerardo, “*Derecho a la intimidad, hábeas data y el derecho a la autodeterminación informativa*”, en *Iustitia*. Año 11, N° 130-131.
- RAMOS, Dirceo Tordecillas. *Remédios constitucionais: hábeas corpus, mandado de segurança, mandado de segurança coletivo, ação popular, ação civil pública, mandado de injunção, hábeas data*. São Paulo: Angelotti, 1993.
- RASI, Gaetano. *Società e Privacy. Un anno da Garante*. Roma: Sallustiana. 2.002.
- VOLIO ECHEVERRÍA, Fabián, *El amparo contra sujetos de derecho privado*, en *Iustitia*. San José, 7(82): 1992.
- ZENO-ZENCOVICH, Vincenzo, *Uso a fini privati del dati personali in mano pubblica. Privacy, da Costo a Ricorsa*. Roma, 2002.

Expedientes legislativos:

- NÚMERO 12827: Proyecto de “Adición de un nuevo capítulo IV, denominado ‘Del Recurso de Hábeas Data’, al título III, de la Ley de la Jurisdicción Constitucional, Ley N° 7135, del 19 de octubre de 1989”, 1996. (El mismo proyecto ha sido presentado en 2.003 con los números 14.778 y 14.785)
- NÚMERO 15.079: Proyecto de “Ley de acceso a la información para la transparencia de la gestión pública estatal. 2.002.
- NÚMERO 15.178: Proyecto de “Ley de protección de la persona frente al tratamiento de sus datos personales”. 2.003.

