La protección de datos: una necesidad

José María Ayala Muñoz* y Celia Fernández Aller**

La sociedad de la información avanza rápida y penetrante en todo el mundo; El Salvador no es la excepción. Ello trae consigo ventajas, sobre todo en lo que se refiere a la capacidad de almacenamiento y transmisión de grandes cantidades de información a velocidad impensable hace años; o también a la posibilidad para comerciar y realizar trámites a través de Internet. Sin embargo, el uso inadecuado de las tecnologías de la información y las comunicaciones conlleva amenazas potenciales para los derechos de los individuos, quienes ven cómo su información personal se distribuye en ámbitos geográficos que, por supuesto, exceden el suyo. Esto implica la pérdida de control del uso que se da a esa información, su destino y de las entidades —públicas o privadas, físicas o jurídicas— a las cuales está dirigida.

En la práctica, existe cada vez más conciencia acerca de la necesidad de proteger a las personas frente a estos riesgos. Sin embargo, el camino que queda por recorrer es largo. A los ciudadanos nos falta sensibilización sobre la importancia de proteger al respecto. Sólo cuando estalla un gran escándalo sobre el manejo de los datos o cuando se les da un tratamiento abusivo que nos concierne de forma muy directa (por ejemplo, negación de un crédito por manejo erróneo de una información sobre una deuda pasada ya cancelada), tomamos conciencia de la necesidad de que la protección de los datos sea un derecho reconocido y regulado suficientemente. A las instituciones públicas y privadas les falta comprender

* Abogado del Estado español ante el Tribunal Supremo en Madrid; y profesor de Derecho Comunitario Europeo en la Universidad Pontificia Comillas de Madrid, España.

** Doctora en Derecho Constitucional, con especialidad en Protección Constitucional de Derechos Fundamentales; y profesora de Derecho Informático en la Universidad Politécnica de Madrid, España. Correo electrónico: cfaller@eui.upm.es.

la importancia de políticas activas en materia de protección de datos personales. Éstas no acaban de entender que el cumplimiento de una normativa de protección de datos puede conseguir una mayor transparencia y respeto a los derechos individuales, y hacer más competitivas a las empresas y más eficaces a las administraciones públicas.

1. Introducción a los conceptos

1.1. El derecho a la protección de datos

El llamado derecho a la protección de datos personales se plantea, ante la revolución tecnológica actual, como un instituto que persigue garantizar a los individuos el control de sus datos personales, así como también el uso y el destino de los mismos para impedir el tráfico ilícito y lesivo de éstos. Los ordenamientos jurídicos de otros países, los pronunciamientos judiciales y los estudios de los autores proponen dos formas para reconocer este derecho: como parte del derecho a la intimidad o como un derecho autónomo.

El derecho a la intimidad protege aquellos aspectos que afectan al ámbito más esencial de la persona (datos sobre creencias, afiliación sindical, raza, salud, etc.). El derecho de autodeterminación informativa, denominado con distintos términos (libertad informática o protección de datos), pretende proteger un ámbito más amplio: la "privacidad". Se trata de un conjunto más global de facetas de la persona, las cuales no son consideradas de manera aislada. Al considerarlas de esta última forma pueden carecer de significado intrínseco, pero cuando son analizadas de forma sistemática, permiten obtener un retrato de la persona, cuyos componentes ésta tiene derecho a mantener en reserva. En el concepto de privacidad podrían incluirse datos patrimoniales, gustos personales, consumo, etc.

Creemos que la regulación del derecho a la intimidad pudiera no resultar suficiente para proteger a la persona. Fundamentalmente, porque ese derecho supone otorgar a la persona *poder para controlar* sus datos. Y no solo los datos íntimos, sino también cualquier otro dato cuyo conocimiento o empleo por terceros pueda afectar sus derechos, sean o no fundamentales; porque el objeto a proteger no debiera ser solo la intimidad individual, sino los datos de carácter personal, ya sean éstos de carácter íntimo o no.

El contenido de este derecho de protección de datos es peculiar, debido a que otorga al titular una serie de facultades, consistentes en poderes jurídicos, cuyo ejercicio impone a terceros deberes jurídicos para garantizar el poder de control. Estos deberes son el derecho a pedir consentimiento previo; a informar en el momento de la recolección de los datos; y a permitir el derecho de acceso, rectificación y cancelación, oposición, indemnización e impugnación de valoraciones arbitrarias. En definitiva, el derecho de autodeterminación informativa concede al sujeto un *poder de disposición*, en virtud del cual decide qué datos proporciona o no; posee la facultad para consentir su registro y la posibilidad de acceso a ellos; controla el uso de los mismos; y le da derecho a ser informado en todo momento acerca de quién dispone de sus datos personales.

1.2. Principales elementos del régimen jurídico

Si se examinan las soluciones dadas por las legislaciones de otros países y los análisis técnico-jurídicos de los especialistas, se concluye que el sistema de protección de datos personales ha de tener un contenido mínimo esencial, necesario para garantizar el respeto a la privacidad y para que el individuo pueda controlar el manejo de sus datos por parte de otra persona o entidad. Hasta ahora, ningún país ha instaurado un sistema completo.

En esta cuestión hay que distinguir dos sujetos. Por un lado, el titular de los datos, es decir, el sujeto cuya información va a ser procesada y a quien se llama "afectado" o "interesado"; por el otro lado, el responsable del procesamiento, quien decide sobre su uso, contenido y finalidad, los cuales pueden ser públicos o privados. En suma, desde el punto de vista doctrinal o científico, los principales

elementos del régimen jurídico del sistema de protección de datos personales son el consentimiento del interesado; los derechos de acceso, rectificación y cancelación de los titulares de los datos; las transferencias internacionales; y el derecho a ser informado antes de otorgar consentimiento.

El consentimiento del interesado, en un sistema que pretenda proteger los datos personales, consiste en prohibir el procesamiento de éstos sin solicitud o aprobación previa de aquél. Será necesaria, por lo tanto, la reserva de ley para exceptuar dicho consentimiento. En el ámbito europeo, las excepciones comprenden la recolección de datos de fuentes accesibles al público, como los medios de comunicación, los repertorios telefónicos, etc.; los datos recogidos en el contexto de una relación de negocios, laboral o administrativa; los datos necesarios para salvaguardar un interés vital del interesado (una urgencia médica, por ejemplo); y los datos utilizados por las administraciones públicas para ejercer sus funciones en el ámbito de su competencia.

Por eso, la exigencia de recabar el consentimiento del interesado carecería de sentido si ella no fuese acompañada de una información previa. Esto es, sólo debe ser válido el consentimiento prestado por quien, debidamente informado, conoce en detalle aquello a lo que consiente. De esta manera, el llamado principio de finalidad supone que, prestado el consentimiento para un determinado tratamiento de los datos, éstos no pueden destinarse a finalidades distintas de las consideradas, bajo pena de considerar nulo el consentimiento. El responsable de recolectar los datos debe informar al afectado, por consiguiente, sobre las finalidades y los usos que va a dar a la información, así como acerca de su localización. La información también permitirá que el interesado pueda ejercer sus derechos y vigilar el cumplimiento de la normativa que protege sus datos.

Para atribuir al afectado un poder de control sobre sus datos, aun después de haber consentido su procesamiento, debe concedérsele derecho para acceder al contenido del fichero y modificar los datos erróneos o cancelarlos cuando dejan de ser necesarios para la finalidad para la cual fueron recogidos. Complemento de esto es considerar los derechos a oponerse al procesamiento; crear un registro centralizado de archivos de tratamiento de datos y de derecho de consulta para que el afectado pueda conocer en cuántos ficheros públicos o privados se encuentra su información; el derecho de indemnización, que permite resarcir, en el caso de daños morales o patrimoniales, derivados de un tratamiento incorrecto de los datos; y el derecho de impugnación de las valoraciones arbitrarias, lo cual impide a terceros tomar decisiones sobre la persona, basadas única y exclusivamente en una valoración de datos personales. En este mismo sentido, debe exigirse al responsable del fichero que el tratamiento se haga con condiciones mínimas de calidad. El principio de calidad impone que el tratamiento de los datos sea adecuado, pertinente y no excesivo en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las cuales se han obtenido.

Puede suceder que, al traspasar las fronteras, los titulares de los datos pierden la posibilidad de controlar su destino. Y si el país receptor cuenta con un nivel de protección de datos inferior al país emisor, los derechos de la persona pueden verse vulnerados. De este modo, para que los derechos hasta aquí expuestos sean eficaces y no puedan ser defraudados por la salida de los datos fuera del territorio nacional del Estado que establece la regulación, deben imponerse limitaciones o restricciones a su exportación.

Existen dos modelos para regular estas transferencias. El modelo estadounidense utiliza los principios de "puerto seguro", establecidos por el Departamento de Comercio el 19 de abril de 1999. Las empresas estadounidenses que quieran contar con el beneficio de "puerto seguro" deben satisfacer unas condiciones mínimas: notificación, opción, transferencia ulterior, seguridad, integridad de los datos, acceso y aplicación. De esta forma, cualquier empresa estadounidense que quiera negociar con una europea ha de cumplir estos

estándares de protección de datos. Sin embargo, este modelo cuenta con muchas limitaciones, tal y como ha detectado el Dictamen 2/99 de la Unión Europea sobre la idoneidad de los "Principios internacionales de puerto de seguro"[1].

Por su parte, el modelo europeo exige, para transferir datos personales a otros países, un tratamiento adecuado, de acuerdo a los criterios siguientes[2]: (a) principio de finalidad; (b) principio de proporcionalidad y calidad de los datos; (c) principio de transparencia; (d) principio de seguridad; y (e) derecho de acceso, rectificación y oposición. Además, existen restricciones para hacer transferencias sucesivas a terceros países: solo se permiten transferencias sucesivas de datos personales del tercer país de destino a otro tercer país en el caso de que este último garantice, asimismo, un nivel de protección de datos adecuado. Este modelo también tiene limitaciones, por ejemplo: cómo definir qué es la "protección adecuada" y cuáles son las excepciones; la diferente regulación entre países; y la cuantía de las sanciones pecuniarias.

1.3. Mecanismos especiales de control

La garantía eficaz de protección de datos de carácter personal no solo exige la declaración legal de los derechos hasta aquí expuestos, sino que también el establecimiento de mecanismos adecuados para —por la vía administrativa y judicial— asegurar una reacción de los poderes públicos contra los actos lesivos a tales derechos. Con este fin, puede crearse un organismo de carácter administrativo, dotado de suficiente autonomía para controlar no solo los ficheros en poder de empresas privadas, sino también en poder de la administración pública.

También existe la posibilidad de reconocer un proceso judicial, el hábeas data. Se trata éste de un remedio constitucional contra los abusos de poder y las ilegalidades cometidas por los servidores o los agentes públicos, y relacionadas con las informaciones y los datos de los administrados. En algunos países, solo se refiere a datos públicos; en otros, incluye los datos de los ficheros de titularidad privada. Normalmente, no se distingue si las bases de datos están o no informatizadas. Este remedio constitucional debe ser activado a instancia de la parte interesada, no de oficio. En algunas constituciones se establece que el sujeto activo y peticionario debe ser el titular de los datos personales; en otras, se faculta, además, a los familiares, en caso de que el titular hubiere fallecido o no pudiere hacerlo.

El procedimiento suele ser breve. Los plazos de presentación de pruebas y alegaciones son cortos y las resoluciones deben hacerse efectivas con prontitud. La tramitación está a cargo de un órgano judicial, para lo cual los tribunales ordinarios o una sala de justicia determinada podrían tener competencia. Sin embargo, el hábeas data, por sí mismo, no garantiza una protección adecuada de los datos. En tanto que su finalidad es corregir irregularidades en el tratamiento de los datos personales, no es un medio idóneo para prevenir acciones que atenten contra los derechos y las libertades; así como tampoco sirve para regular cómo debe ser tratada la información. De hecho, de los seis principios del documento del Grupo de Autoridades Europeas de Protección de Datos (GT29), el hábeas data incluye solo el quinto (y de modo parcial).

1.4. Exclusiones de la normativa de protección de datos

En ciertas ocasiones, el bien jurídico protegido por estas normas, la privacidad de individuo, ha de ceder ante razones de interés público. Dentro de estas razones estarían el mantenimiento de la seguridad nacional e internacional, la lucha contra el terrorismo, etc. En todas las normativas de protección de datos, se establecen excepciones en el ámbito de aplicación. Así, en el Artículo 2.2 de la ley

1. Disponible en http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp19es.pdf.
2. El Grupo de Autoridades Europeas de Protección de Datos (GT29) estableció dichos criterios.

española de protección de datos se excluyen tres supuestos: ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas; ficheros sometidos a la protección de "materias clasificadas"[3]; y ficheros para la investigación del terrorismo y formas graves de delincuencia organizada. Asimismo, la Directiva 95/46 de la Unión Europea sobre protección de datos de las personas físicas[4] establece excepciones —a los derechos de información y acceso, y a algunos principios— en su Artículo 13:

> 1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de:
>
> a) la seguridad del Estado;
>
> b) la defensa;
>
> c) la seguridad pública;
>
> d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;
>
> e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;
>
> f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e);
>
> g) la protección del interesado o de los derechos y libertades de otras personas.

2. La necesidad de regular la protección de datos personales

Al abordar la cuestión de la libertad informática en El Salvador, surge una primera interrogante: ¿cuál es la pertinencia de ocuparse de ello en un país que tiene otras muchas necesidades y carestías de orden jurídico, social o económico? Dados estos problemas, ¿qué razón habría para ocuparse de la protección de datos personales? Pareciera que antes de proteger los datos personales habría que resolver la inseguridad ciudadana, la pobreza, la estabilidad jurídica o incluso la erradicación de la corrupción. Sin embargo, una vez conocida la razón de ser y la finalidad de la libertad informática y la protección de datos personales, una vez reconocido que se trata de un derecho fundamental de la persona, la respuesta a estas cuestiones es inmediata, puesto que los salvadoreños son titulares de los mismos derechos fundamentales que las demás personas. No habría, por lo tanto, razón alguna para que el Estado y el legislador no concedan el mismo respeto y la misma dignidad a la población salvadoreña que aquella de la cual goza la europea, la australiana o la canadiense. ¿O es que la protección de la intimidad o de la libertad informática impide otros avances o entorpece, dificulta o retrasa otros procesos prioritarios para El Salvador?

El Salvador tiene, sin duda, carencias, al igual que otros países que aparentemente han avanzado más. Pero los salvadoreños, y su poder público, se desarrollan en la misma época y, en muchos aspectos, en condiciones muy similares a las de los demás países. De esta manera, así como atiende sus necesidades más específicas, también debe ocuparse, al mismo tiempo que los demás países, de los problemas actuales que le son comunes. En El Salvador, la libertad informática y la protección de los datos personales no solo son un problema que debe ser atendido tal como en el resto de naciones, sino que, además, su regulación es esencial para tratar otros problemas prioritarios.

La protección de la dignidad de las personas y de su intimidad, que constituyen valores básicos del derecho salvadoreño y presiden su constitución, exigen, en la era de las nuevas

3. "Asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas puede dañar o poner en riesgo la seguridad y defensa del Estado".
4. Disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:HTML.

tecnologías, regular la libertad informática. No se trata de que se hayan detectado nuevos valores dignos de ser protegidos y que exijan nuevas normas. Si este fuera el caso, habría razones para sostener que antes de proteger estos nuevos valores o estas nuevas necesidades, es necesario satisfacer otras necesidades básicas. Más bien se trata de que la protección de las necesidades básicas exige asegurar la protección de datos personales y la libertad informática. En efecto, la protección de la dignidad de la persona o de su intimidad (valores que no son nuevos ni superfluos, sino básicos en cualquier comunidad social) exigía unas determinadas medidas hace cincuenta años, y requiere de otras medidas, adaptadas a los tiempos modernos, en la actualidad. Por ejemplo, sin una adecuada protección de los datos personales, muchas personas tendrían miedo a ejercer derechos como la sindicación o la participación activa en la vida política del país, puesto que existe la posibilidad de que el Estado o determinados grupos de poder puedan controlar estas actividades y adoptar represalias o medidas coercitivas contra ellas.

Pero la seguridad ciudadana salvadoreña está amenazada no solo por problemas particulares del país, sino también por problemas más generales, como la lucha contra el crimen organizado en los ámbitos nacional e internacional. Esta lucha exige una serie de medidas de control que solo pueden compaginarse con un Estado de derecho si están acompañadas por una regulación apropiada que proteja los datos. En efecto, las medidas de control de datos exigidas por la lucha contra el terrorismo, el narcotráfico o las bandas delincuenciales no serán legítimas si no van acompañadas de las garantías pertinentes para proteger los derechos fundamentales de las personas. La necesaria compatibilidad entre la eficacia policial y el respeto a los derechos humanos solo es posible si se presta atención a la regulación de la protección de los datos personales y las garantías ciudadanas.

Prueba de este argumento es la polémica que se suscitó en la Unión Europea a propósito de la aprobación de una norma que obliga a las operadoras de telefonía y a los servidores de Internet a almacenar los datos (no los contenidos) de todas las comunicaciones electrónicas y telefónicas por lo menos durante un año[5]. La finalidad de la norma, obviamente, es contribuir a que la lucha contra el terrorismo sea más eficaz, pero sin retroceder en los logros alcanzados en materia de derechos humanos. De otro modo, el terrorismo, al igual que otras formas de crimen organizado, conseguiría, en parte, sus fines, pues su combate llevaría a un retroceso social de los avances jurídicos y sociales, y se limitaría el ejercicio de los derechos humanos.

Otro aspecto relevante asociado a la cuestión es la transparencia pública. En El Salvador, el consenso en torno a necesidad de la transparencia pública es bastante amplio, pues ésta facilita la actividad de las empresas y, en general, de toda la sociedad civil salvadoreña. Sin duda, garantizarla e implementarla aumentaría la confianza de la ciudadanía en las administraciones públicas y fortalecería el Estado social, democrático y de derecho en el país. La protección de datos coadyuva a la transparencia pública en la medida que, al permitir al ciudadano controlar el uso de sus datos personales, abre la posibilidad de acceder al contenido de los ficheros públicos y privados. De esta manera, la protección de datos permite a las personas ejercitar el derecho de acceso a determinado tipo de información pública.

En el derecho comparado, y fundamentalmente en los países más desarrollados, existe ya una regulación, más o menos precisa, de la libertad informática y de la protección de datos personales. Del mismo modo, los Estados de las economías más poderosas han establecido normas para regular el movimiento de datos fuera de sus fronteras. El propósito de estas normas es impedir que los datos protegidos puedan llegar a países que, como El Salvador

5. Las implicaciones técnicas del problema no están solucionadas, pues, como se sabe, los procesos de encriptación de los correos pueden evadir todo tipo de cautelas legales.

actual, no cuentan con una regulación y unas garantías para proteger los datos de carácter personal.

En este sentido, y solo por señalar los casos más significativos, la Directiva de la Comunidad Europea 95/46/CE establece que no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal hacia países que no proporcionen un nivel de protección equiparable al de la regulación europea, aunque con excepciones específicas, previstas por la misma normativa comunitaria europea. Por su parte, el Departamento de Comercio de Estados Unidos hizo públicos unos "principios internacionales de puerto seguro", los cuales sirven de punto de referencia a las empresas estadounidenses que desean garantizar las exigencias de "protección adecuada"[6].

Por otra parte, las necesidades del comercio, en un mundo globalizado como el actual, pueden exigir que El Salvador, al igual que otros países de su entorno, adopte una regulación para proteger los datos personales si quiere evitar un eventual bloqueo de la transferencia internacional de datos a sus empresas, lo cual entorpecería su expansión o su desarrollo comercial. Además, las pretensiones de integración económica de El Salvador exigen armonizar las legislaciones sobre estos temas. En la Unión Europea, la unión económica y monetaria se ha visto facilitada por la aproximación de las normativas a través de las directivas de protección de datos. Tal y como dice la Sala de lo Constitucional de Costa Rica, "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 de otros ciudadanos"[7].

Las principales razones que motivan a las empresas de los países desarrollados a regular la protección de datos son varias[8]. En primer lugar, la mejora de la imagen y de la percepción de seguridad por parte de clientes y empleados. Esta mejora supone un valor añadido a sus servicios. Desde una perspectiva social y de atención al cliente, los esfuerzos de una empresa para adecuarse a la normativa son perceptibles en los contratos, donde se insertan cláusulas específicas al respecto; en la gestión eficaz de los derechos de acceso; en la rectificación, cancelación y oposición de los clientes; en el envío de cartas con diferentes fines con leyendas relativas a la protección de datos; en el uso de un protocolo seguro en la página web institucional, etc. También resulta importante generar un sentimiento de seguridad entre los empleados con respecto a sus propios datos personales. En España, por ejemplo, la Agencia de Protección de Datos impide a las empresas que forman parte de un grupo compartir datos, a no ser que el interesado dé su consentimiento.

En segundo lugar, la mejora de la gestión y de los procedimientos internos en el marco de un proceso más global, dirigido a reconstruir la estructura organizativa y técnica de la entidad por motivos como los siguientes: ganar agilidad en los procesos y en la atención al cliente; cumplir con otras normas; cambios en

6. A su vez, la Unión Europea y Estados Unidos han llegado a acuerdos de "puerto seguro", como el recogido en la Decisión de la Comisión de las Comunidades Europeas del 26 de junio de 2000 (2000/520/CE) "sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América". En este sentido, también debe citarse la Decisión de la Comisión de las Comunidades Europeas del 30 de junio de 2003 (2003/490/CE), que reconoce que la legislación argentina ofrecía un nivel de protección de datos adecuado. Ambas disponibles, respectivamente, en http://peru.cpsr.org/bdatos/decisiones/europa/Decision2000_520_CE_PuertoSeguro.pdf y http://peru.cpsr.org/bdatos/decisiones/europa/Decision2003_490_CE_Argentina.pdf.
7. Chirino Sánchez, A., "El recurso de 'habeas data' como forma de tutela de la persona frente al tratamiento de sus datos personales. El caso de Costa Rica", IX Congreso Iberoamericano de Derecho e Informática "Justicia e Internet", enero de 2002. Disponible en http://hess-cr.com/secciones/cursos/uned/dersfund/chirino.rtf.
8. Ver Ecija Abogados, *Factbook. Protección de datos personales*, Navarra: Editorial Aranzadi, 2003, p. 203.

el organigrama; proceso de fusión o absorción con otra entidad; sistemas y aplicaciones obsoletas, etc. Y, en tercer lugar, la mala imagen que producen las sanciones del organismo que vela por la garantía de la protección de datos. Con independencia de la dimensión de la empresa y del volumen de sus actividades, el daño social que puede causar la noticia de la sanción puede ser mucho mayor.

Finalmente, otra línea argumentativa para justificar la necesidad de regular la protección de datos personales tiene que ver con la mejora de los índices de desarrollo humano y social. Nuestra tesis es que las tecnologías de la información y la comunicación pueden suponer fracturas digitales y exclusión, amenazas a las libertades. Sin embargo, equitativamente utilizadas también pueden contribuir a elevar los índices de desarrollo humano (medición del nivel de vida digno, longevidad y conocimientos) y desarrollo social. Sin duda, las tecnologías de la información y la comunicación abren mayores posibilidades para la participación social y política[9], lo cual contribuye a este desarrollo social. Además, varios estudios demuestran que la inversión en la tecnología de la información tiene un efecto multiplicador en el crecimiento económico. Por su lado, los Objetivos de Desarrollo del Milenio, en concreto el 8 ("Fomentar una asociación mundial para el desarrollo"), establecen la necesidad de que, en coordinación con el sector privado, las nuevas tecnologías se hagan asequibles a todos y todas, especialmente los beneficios de la informática y las telecomunicaciones. Estos objetivos para el desarrollo fueron pactados en el marco de un consenso muy global.

3. Derecho comparado

Desde la perspectiva del derecho comparado, es importante considerar —aunque sea de manera muy breve— la situación de Estados Unidos, la Unión Europea y de otros países con los cuales El Salvador mantiene relaciones comerciales y culturales; pero sobre todo conviene tomar en cuenta la situación de los demás países latinoamericanos.

En Estados Unidos, el control de los ficheros de las empresas se fundamenta en un sistema de autorregulación, mientras que el de los ficheros de titularidad pública es objeto de regulación legal. De este modo, se garantiza la protección de datos de carácter personal, aunque a un nivel muy inferior al concedido en la regulación europea. En la Unión Europea, la protección de datos personales pertenece al ámbito comunitario. Es así como la regulación de todos y cada uno de los Estados miembros se adaptó a las exigencias de las directivas de la Unión Europea[10]. Éstas norman la necesidad del consentimiento del interesado; los derechos de información, acceso, rectificación, cancelación y oposición; la transferencia internacional de datos; e imponen a cada Estado la obligación de crear un órgano independiente de control y un registro de ficheros públicos y privados. Por supuesto, se excluyen de la regulación, o se someten a reglas especiales, los ficheros relacionados con la defensa nacional, la seguridad pública u otros, cuyas circunstancias especiales ameritan una excepción. El modelo europeo se ha extendido a Australia, Nueva Zelanda, Canadá, Taiwán, Hong Kong y Japón, entre otros países.

En general, en América Latina la regulación es mucho más avanzada y detallada que la de El Salvador. En efecto, desde los primeros años de esta década, todos los Estados latinoamericanos se han esforzado —a iniciativa de la Agencia Española de Protección de Datos— por crear una Red Iberoamericana de Protección de Datos de carácter personal. Asimismo, todos ellos acordaron progresar en este campo. Este compromiso está recogido, por ejemplo, en la Declaración de La Antigua (II Encuentro Iberoamericano de Protección de Datos

9. Piénsese en la democracia electrónica y en los conceptos de voto electrónico y telemático.
10. Directiva 95/46 del 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; y Directiva 02/58/CE del 12 de julio de 2002, que versa sobre la protección de datos personales en el ámbito de las comunicaciones electrónicas.

Personales), que establece lo siguiente: "Se constata la necesidad de impulsar la adopción de medidas que garanticen un elevado nivel de protección de datos, así como la idoneidad de contar con marcos normativos nacionales que, inspirados en tradiciones jurídicas comunes [...] garanticen una protección adecuada". Además, en la Declaración de Cartagena de Indias (III Encuentro Iberoamericano de Protección de Datos) se concluye que "el tratamiento leal, lícito, transparente y ético de datos personales constituye una garantía de la persona que debe ser respetada en la búsqueda de objetivos como velar por la estabilidad del sistema financiero y facilitar el acceso al crédito".

Varios países latinoamericanos han promulgado o están en vías de promulgar normas más o menos avanzadas en materia de protección de datos de carácter personal. En este sentido, y con el simple ánimo de dar una idea general, ha de decirse que cuentan con una ley sobre protección de datos de carácter personal, Argentina (cuya regulación es equiparable a la de la Unión Europea), México, Chile, Paraguay y Venezuela. Tienen proyectos de ley en fases más o menos avanzadas, Costa Rica, Perú y Brasil. Y cuentan con una previsión constitucional específica del hábeas data, Colombia, Brasil, Argentina, Perú, Uruguay y Ecuador.

4. La situación en El Salvador

En El Salvador existen circunstancias muy oportunas para regular la protección de datos personales. Esto es, no solo deben considerarse las razones que, en general, justifican una regulación para la protección de estos datos, sino también otras razones que, en particular, hacen necesaria esa regulación en el país. En este sentido, cabe traer a cuenta los pronunciamientos de la Sala de lo Constitucional de la Corte Suprema de Justicia que afirman, de manera concluyente, que la Constitución garantiza la protección de datos personales. La Corte admitió a trámite un recurso que plantea desarrollar los mecanismos legales idóneos para la protección del derecho a la autodeterminación informativa, en los términos que se pasa a exponer.

El planteamiento sostiene que el inciso primero del Artículo 2 de la Constitución afirma: "Toda persona tiene derecho a la vida, a la integridad física y moral, a la libertad, a la seguridad, al trabajo, a la propiedad y posesión, y a ser protegida en la conservación y defensa de los mismos". En el segundo inciso añade: "Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen". La jurisprudencia salvadoreña[11] ha considerado que el Artículo 2 de la Constitución pudiera determinar la necesidad de desarrollar legislativamente los mecanismos y las garantías para la conservación y defensa del derecho a la autodeterminación informativa. Así, en resolución del 15 de febrero de 2005, establece que "el derecho a la autodeterminación informativa tiene un contenido constitucionalmente definido compuesto por una diversidad de facultades relacionadas; la falta de desarrollo legislativo no afecta a ese contenido constitucional, sino que puede incidir —lo cual habrá de determinarse en el pronunciamiento de fondo de este proceso— en la falta de garantías legales que le doten de eficacia". Dicha resolución termina admitiendo la demanda presentada, "en cuanto a la supuesta inconstitucionalidad en que incurre la Asamblea Legislativa, en tanto que no ha desarrollado legalmente los mecanismos idóneos de protección del derecho a la autodeterminación informativa, mandato constitucional derivado de la integración de los incisos 1º y 2º del artículo 2 de la Constitución".

Las instituciones salvadoreñas, públicas y privadas, se han mostrado abiertas y receptivas al tema. Sin embargo, en la práctica, son pocas las acciones que confirman esa apertura discursiva. Hasta 2005, se registran ciertas regulaciones sectoriales, como la normativa que regula la Ley Penitenciaria (la cual alude a los datos personales de los reclusos) o la mo-

11. Sentencia del 2 de marzo de 2004 (proceso de amparo constitucional 118-2002); Resolución del 15 de febrero de 2005 (proceso de inconstitucionalidad 36-2004).

dificación, en diciembre de 2005, del Código Municipal[12] a instancias de la Corporación de Municipalidades de El Salvador (COMURES) y diversas organizaciones de la sociedad civil. A raíz de dicha reforma, en el Título IX del Código ("De la participación ciudadana y de la transparencia") se establece lo siguiente:

> Art. 125-A.- Se entenderá por transparencia en la gestión municipal a las políticas y mecanismos que permiten el acceso público a la información sobre la administración municipal.
>
> Art. 125-B.- Todos los ciudadanos domiciliados en el municipio tienen derecho a:
>
> a) Solicitar información por escrito a los Concejos Municipales y a recibir respuesta de manera clara y oportuna;
>
> b) Ser informados de las decisiones gubernamentales que afecten al desarrollo local;
>
> c) Conocer el funcionamiento del Gobierno Municipal y del manejo de su administración;
>
> d) Ser tomados en cuenta por las autoridades municipales en la aplicación de las políticas públicas locales;
>
> e) Recibir informe anual de rendición de cuentas y ejercer contraloría a través del comité respectivo, en la ejecución de obras de infraestructura.
>
> Art. 125-C.- La municipalidad tiene la obligación de:
>
> a) Garantizar el ejercicio de los derechos a que se refiere el Art. 125-B;
>
> b) Informar a los ciudadanos de su comprensión lo pertinente a la administración municipal, en forma clara, oportuna y actualizada;
>
> c) Proporcionar la información requerida por los ciudadanos cuando sea procedente de acuerdo a este Código.
>
> Art. 125-D.- La información de acceso público a que se refiere el presente Capítulo, será la contenida en los documentos siguientes:
>
> a) Ordenanzas municipales y sus proyectos;
>
> b) Reglamentos;
>
> c) Presupuesto Municipal;
>
> d) Planes municipales;
>
> e) Valúo de bienes a adquirir o vender;
>
> f) Fotografías, grabaciones y filmes de actos públicos;
>
> g) Actas del Concejo Municipal;
>
> h) Informes finales de auditoría.

Por otro lado, la Ley de Protección al Consumidor del 18 de agosto de 2005[13], en el apartado dedicado a las "Obligaciones de entidades especializadas en la prestación de servicios de información", establece:

> Art. 21.- Las entidades especializadas en la prestación de servicios de información estarán obligadas a permitir al consumidor el acceso a la información de sus datos, así como a solicitar la actualización, modificación y eliminación de los mismos, de forma gratuita.
>
> Asimismo, tendrán la obligación de corregir la información falsa, no actualizada o inexacta en un plazo máximo de diez días contados a partir de la recepción de la solicitud del interesado.
>
> Las entidades especializadas a las que se refiere el presente artículo, no podrán obtener ninguna clase de información personal del consumidor, si no es con la debida autorización de éste, y únicamente en las condiciones en que la misma haya sido conferida.

Sin una regulación adecuada, se produce un vacío normativo. Ello implica que las empresas que en otros países operan de acuerdo a los principios de regulación de datos, en El Salvador trabajan con criterios diferentes. Esta falta de regulación deja al ciudadano en una gran indefensión. Por este motivo, no debería hacerse una regulación sectorial del tema (por ejemplo, solo de los ficheros bancarios y la información a éstos), sino una integral: una ley de protección de datos que comprenda todos los ficheros que tratan información personal, tanto de forma manual como informatizada.

12. Disponible en http://www.csj.gob.sv/leyes.nsf/0/1db8b637a047a63c06256d02005a3af3?OpenDocument.
13. Disponible en http://www.defensoria.net/uploaded/content/category/1970757648.htm.

Sin embargo, es esperanzador que la vinculación entre la tutela de los datos personales y el desarrollo de la sociedad de la información haya sido percibida como importante por el propio Gobierno salvadoreño. Éste apuesta por el uso de nuevas tecnologías y su regulación, tal como se establece en la *Estrategia nacional de gobierno electrónico*[14], formulada por la Secretaría Técnica de la Presidencia (febrero de 2004). En el documento se señala que "El concepto de Gobierno Electrónico [...] trata de una reforma de Estado, mucho más ambiciosa, que busca transformar la forma en la que el Gobierno se relaciona con los ciudadanos, la empresa privada y las diversas organizaciones de la sociedad, por medio de un cambio radical en la gestión administrativa que fomente la eficacia y transparencia en la interacción del Gobierno con sus usuarios" .

5. Alternativas de regulación[15]

El Salvador carece de un marco normativo sobre el acceso a la información pública o privada, y sobre el régimen de protección de datos, pese a que existen numerosos registros, públicos y privados, informáticos y manuales, que contienen información personal. Regular esta información permitiría desarrollar en El Salvador la sociedad de la información y, dentro de ella, todo lo relacionado con el comercio electrónico.

Existen muchas alternativas para la regulación de la libertad informática. En el ámbito doctrinal se pueden crear leyes de protección de datos, siguiendo el modelo europeo; implementar en el sector público las directrices de la Organización para la Cooperación y el Desarrollo Económico (con un simple decreto que liste su contenido en un anexo), y promover su adopción; en el sector privado, a través de uniones industriales y cámaras empresariales, como paso previo a la aprobación de la ley; promover un convenio latinoamericano al estilo del Convenio No. 108 del Consejo de Europa (podría realizarse a nivel del Pacto de San José de Costa Rica o la Organización de Estados Americanos); promover la creación de organismos rápidos, flexibles y no burocráticos, con facultades sancionadoras y reglamentarias, en materia de protección de datos para evitar abusos del poder informático; y reglamentar el hábeas data a niveles constitucional y procesal como herramienta efectiva para controlar los datos personales. De esta manera, se posibilita el desarrollo pleno del individuo y su protección en la sociedad tecnológica.

Por otra parte, es necesario armonizar la legislación nacional con la del entorno en el campo de la libertad informática. En particular, es indispensable armonizar la legislación salvadoreña con la de Iberoamérica. No es lo más adecuado que el derecho de la protección de datos se derive de un desarrollo posterior del fallo de la Sala de lo Constitucional. No obstante los esfuerzos hechos hasta ahora para modernizar el sistema judicial salvadoreño, el amparo como instrumento para defender los derechos fundamentales no es tan eficaz como parece. La jurisprudencia matiza y complementa la letra de la ley, pero nunca puede llegar tan lejos como para desarrollar el contenido de un derecho nuevo.

El Salvador tiene buenos ejemplos de regulación legislativa en el continente latinoamericano: Estados Unidos, Canadá y Argentina. De sus leyes y resoluciones jurisprudenciales pueden extraerse los elementos principales para un derecho de cuarta generación, cuyos perfiles están definidos en numerosas leyes y documentos internacionales. En efecto, existe ya un consenso internacional amplio acerca de

14. Disponible en http://www.elsalvador.gob.sv/pge/estrategia.pdf.
15. Estas conclusiones se desprenden del estudio monográfico sobre esta cuestión (Ayala Muñoz, J. M., Campos, H., Corripio, R., Rodríguez, R. y Fernández Aller, C., *La protección de datos personales en El Salvador*, San Salvador: UCA Editores, 2005), elaborado en el marco del proyecto de cooperación interuniversitaria *Situación de la libertad informática en El Salvador. Hábeas data y transmisiones internacionales de datos.* Dicho proyecto contó con la participación de las universidades Centroamericana "José Simeón Cañas" (UCA) de El Salvador; Politécnica de Madrid; y Comillas de Madrid. La financiación provino de la Agencia Española de Cooperación Internacional y de la Universidad Politécnica de Madrid.