Hacia un modelo integrado de regulación y control en la protección de los datos personales

ALBERTO CERDA SILVA*
UNIVERSIDAD DE CHILE

Resumen: el artículo que a continuación se presenta realiza una revisión de los sistemas de regulación y control de datos personales; desde un sistema de heterorregulación o heterocontrol, basados en una autoridad pública de control, a un sistema de autorregulación o autocontrol, cuyas manifestaciones son el modelo de normas de conducta, en que los propios actores relevantes adoptan normas en lo concerniente al tratamiento de los datos personales; y el agente de control interno, basado en un encargado de tratamiento, quien es nombrado por el responsable del tratamiento para cerciorarse de que las operaciones efectuadas no atentan contra los derechos y libertades de los interesados. Además se prevé la presencia de un sistema integrado, que reúne técnicas de control y de regulación.

Palabras clave: Tratamiento de Datos, Bases de Datos, APEC Privacy Framework.

Abstract: The article that it is presented make a review of the regulation systems and the control of personal data, from a system of 'hetero-regulation' o 'hetero-control', based in a control public authority, to a system of 'auto-regulation' o 'auto-control', which manifestations are the behavior`s norm model, in which the own relevant actors adopt norms relating to the treatment of personal data; and the inner control agent, based in a treatment person in charge, whom is designated by the responsible of the treatment to be sure of the made operations do not attempt against rights and liberties of the interested. Also, it is foresee the presence of an integrated system, that satisfy the techniques of control and of regulation.

Keywords: Data treatment, Data Bases, APEC Privacy Framework.

1.- Introducción

Aun cuando la realidad supera con creces las pretensiones de un modelo, cuyo artificio consisten en llevar a una simplificación de la realidad, estos representan utilidad cuando se le atribuyen una simple pretensión explicativa. En materia de protección de los derechos de las personas, en relación con el tratamiento de los datos personales, es posible sostener la existencia de pautas comunes entre

* Abogado y Magíster en Derecho Público por la Universidad de Chile. Profesor Asistente de Derecho Informático e Investigador del Centro de Estudios en Derecho Informático de la Universidad de Chile. acerda@uchile.cl

diversas expresiones normativas sobre las cuales construir ciertos modelos en materia de regulación y control.

En lo que sigue, procuraremos sostener la existencia de dos modelos bastante distintos, pese a los elementos comunes habidos entre uno y otro, en cuanto a la regulación y control en la protección de las personas respecto del tratamiento de los datos personales que les conciernen. Profundizaremos sobre dos mecanismos: uno de autorregulación, los códigos de conducta, y otro de autocontrol, al que hemos denominado agente de control interno.

Finalmente, tras constatar que los modelos mencionados no resultan químicamente puros, avanzaremos en la descripción de un modelo integrado o híbrido, en el cual se observa una mixtura de mecanismos de regulación y control, mediante lo cual se obtiene una adecuada protección de los derechos de las personas concernidas, junto con evitar un entorpecimiento al flujo de datos personales que intervenga indebidamente el funcionamiento de los mercados.

2.- Modelos de regulación y control

2.1.- Modelo de heterorregulación y heterocontrol

Inicialmente, cuando el número y costos asociados al funcionamiento de equipamiento computacional suponían su empleo sólo por grandes reparticiones públicas, tiene lugar la promulgación de la primera legislación en la materia. Así, en 1973 Suecia adopta la Ley de Datos, por la cual imponía un sistema de registro abierto para publicitar los bancos de datos personales relativo a personas físicas realizado por medios automatizados, los que debían ser previamente autorizados para funcionar por la autoridad pública. Una autoridad de control –la Inspección de Datos, expresión del *Ombudsman* proyectado al tratamiento de datos– velaba por el respeto de la ley, con facultades inspectoras, normativas y procesales para requerir la aplicación judicial de sanciones.

Esta primera legislación se caracterizó por centrar la protección en una reglamentación de las bases de datos, imponiendo ciertas restricciones a su constitución, tales como sistemas de autorización, inspecciones previas, etc. Además, en ella se contemplaba entidades de naturaleza administrativa encargadas de velar por el cumplimiento de la normativa, con facultades de fiscalización tanto a la época de constitución de la base, como durante su operación.

El modelo regulatorio y de control previsto en la normativa sueca se sustentaba fundamentalmente en el cometido de la autoridad pública y dejaba escaso margen de maniobra para la adopción de normas y mecanismos de control por los propios actores relevantes; de hecho, en ellas se observa un reconocimiento bastante incipiente de los propios derechos de los titulares de datos personales, mediante los cuales abogar por el cumplimiento de la normativa aplicable.

Si bien el sustrato de la actual normativa de la Unión Europea se encuentra en este modelo, lo cierto es que se ha admitido, según lo que veremos posteriormente, un importante cometido de parte de los propios titulares de derechos y responsables de tratamiento en la regulación y control en la materia; la explicación de ello radica parcialmente en el crecimiento exponencial de los sistemas de información, lo que hace imposible verificar una adecuada regulación y control mediante el único expediente de una autoridad pública.

2.2.- Modelo de autorregulación y autocontrol

En contrapartida al modelo precedente, tenemos aquél que releva a los actores involucrados, empoderándolos en la regulación y control del adecuado de tratamiento de los datos personales. Es el caso de Estados Unidos y Chile. Es también el rasgo distintivo de APEC Privacy Framework.

No se trata, contrariamente a lo que se pudiera pensar, de una absoluta prescindencia estatal en relación con los problemas propios del tratamiento de los datos personales. De hecho, tanto en un modelo como en otro los Estados han reglamentado legalmente el tratamiento de tales datos y, por supuesto, siempre es posible recurrir a la autoridad judicial para obtener la resolución de los conflictos suscitados en relación con tal normativa.

La diferencia entre el modelo precedente y este último radican en que para ciertos Estados la efectiva tutela frente a los riesgos de la informática exige una intervención adicional del Estado, de un organismo público independiente encargado de promover e informar sobre la legislación en cuestión, fiscalizar el cumplimiento de ella y sancionar su infracción, o bien instar por la sanción del infractor, en su caso.

El distingo entre un modelo u otro radica en la adopción de un quehacer cotidiano de parte del Estado que evidencie su inequívoco interés en el efectivo cumplimiento de las normas, particularmente cuando ellas están destinadas a salvaguardar intereses difusos, cuyo es el caso tratándose de la legislación de protección frente a los riesgos inherentes al tratamiento de datos personales.[1]

En Estados Unidos, el sistema normativo es fragmentario y está conformado por un farragoso entramado de normas que regulan el tratamiento de datos personales, que descansa en la filosofía de entregar el resguardo del cumplimiento de la normativa a los propios sujetos que intervienen en él, ya sea mediante el control individual ejercido por el titular de los datos –a través del ejercicio de los derechos de información, acceso y rectificación, y la posibilidad de accionar ante tribunales, si es del caso–, o bien de la entidad responsable de tratamiento, mediante la adopción de códigos de conducta y disposiciones reglamentarias, entre otras medidas conducentes a un adecuado tratamiento de los datos.[2]

El sistema promovido por Estados Unidos es objeto de serios cuestionamientos en su seno; junto a un creciente rechazo al actual estado de desarrollo de la protección de la privacidad –especialmente de los datos personales– y repudio de su enfoque esencialmente mercantilista, se ha abogado por la creación de un organismo federal que coordine la protección de la privacidad a nivel nacional como en el extranjero, o bien, en su defecto, cuando menos encargar a alguna entidad existente todas las políticas relacionadas con la materia.[3]

En el caso de Chile, si bien se dispone de una ley general que reglamenta el tratamiento automatizado y no de los datos personales concernientes a personas físicas, la cual prevé derechos y obligaciones para las partes, así como una acción procesal específica, se carece de una autoridad pública que

---

[1] CERDA, Alberto, "La autoridad de control sobre protección de datos personales", en *Anales de la Facultad de Derecho*, Santiago, Universidad de Chile, núm. 2, 2005, pp. 35 – 68.

[2] A modo meramente ejemplar pueden mencionarse, entre otras disposiciones federales y estatales, los siguientes cuerpos legislativos: Privacy Act (1974), Cable Communications Policy Act (1984), Driver's Privacy Protection Act, Electronic Communications Privacy Act (1986), Electronic Funds Transfer Act, Telecommunications Act (1996), Fair Credit Reporting (1970) y Consumer Credit Reporting Reform Act (1996), Right to Financial Privacy Act, Telephone Consumer Protection Act, Video Privacy Protection Act, y Aviation and Transportation Security Act (2001).

[3] SHAPIRO, Andrew, *The control revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know,* Public Affairs/The Century Foundation, 1a. ed. en ingles, 1999, *El mundo en un clic,* traducción de Francisco Ramos, Grijalbo. Barcelona (2001), pp. 259 – 268, 348 – 351.

vele por el cumplimiento de la normativa. Tan sólo se ha previsto una autoridad registral en relación con los organismos del sector público que tratan estos datos.

La omisión de una autoridad pública de control no sólo ha despertado el reparo de la doctrina nacional y extranjera. Con motivo de las negociaciones que precedieron a la suscripción del Acuerdo de Asociación Política, Económica y de Cooperación entre la Unión Europea y Chile, aquélla formuló prevenciones respecto del régimen legal aplicable en el país, siendo las más sustanciosas tres: la carencia de una norma que proscriba la adopción de decisiones de relevancia jurídica respecto de persona determinada sobre la única base de datos tratados automatizadamente; la ausencia de disposiciones especiales aplicables a la transmisión transfronteriza de datos personales que aseguren un nivel de protección adecuado a aquéllos que circulan entre los países partes del Acuerdo; y, la omisión de una autoridad pública independiente que vele por el cumplimiento de la normativa nacional en la materia.

Por su parte, Asia-Pacific Economic Cooperation (APEC) es un foro multilateral de negociación en temas relativos al intercambio comercial, coordinación y cooperación entre las economías de los países que le integran, orientado a promover y facilitar el comercio, las inversiones, la cooperación económica y técnica entre los mismos. Creado en 1989, hoy incluye países como Australia, Canadá, Corea, Chile, China, Estados Unidos, Filipinas, Indonesia, Japón, México, Nueva Zelanda, Perú, Rusia y Vietnam, entre otros.

APEC Privacy Framework es el documento marco para la regulación del tratamiento de la información personal adoptado por las economías que integran APEC, mediante el cual se procura el establecimiento de un estándar de protección que no implique trabas para el comercio internacional entre los países concernidos.[4]

APEC Privacy Framework enfatiza las facultades normativas y de control de que deben gozar las propias entidades responsables del tratamiento de datos y mira con recelo la intervención de una autoridad pública en la materia, por cuanto podría entorpecer el comercio entre las economías involucradas. De hecho, el estándar de protección previsto en APEC es menor al alentado por la Organización de Cooperación y Desarrollo Económicos en su Recomendación de 1980.[5]

En lo que sigue consideraremos brevemente los códigos de conducta y el agente de control interno, dos típicos mecanismos de autorregulación y autocontrol, sus ventajas e inconvenientes, para enseguida sustentar la conjugación de éstos con una autoridad pública independiente que vele por el cumplimiento de la ley, en lo que hemos denominado un modelo integrado.

3.- Mecanismos de autorregulación: códigos de conducta

Cuando nos referimos a mecanismos de autorregulación, aludimos a aquellos en que los propios actores relevantes adoptan normas en lo concerniente al tratamiento de los datos personales. De entre ellos, los más usuales en el derecho comparado son los códigos de conducta, si bien reciben diversa denominación, asociadas a su ámbito de aplicación, tales como códigos de buenas prácticas, códigos de conducta, códigos tipo o políticas de privacidad, entre otras.

Los códigos de conducta constituyen normas de comportamiento adoptadas por los propios destinatarios de sus previsiones, ya se trate de sectores empresariales, asociaciones gremiales o profesionales.[6]

---

[4] *APEC Privacy Framework* fue adoptado en la 16a Reunión Ministerial de APEC, celebrada en Santiago de Chile entre el 17 y 18 de Noviembre de 2004.

[5] *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Recomendación del Consejo de la OCDE, de 23 de septiembre de 1980, y su anexo *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.*

[6] ORTI Vallejo, Antonio, *Derecho a la intimidad e informática*, Ed. Comares, España (1994), p. 17.

Mediante los códigos de conducta se logra familiarizar a sus destinatarios con la legislación y reglamentos vigentes, se inducen al respeto de la ley y se enfrenta la obsolescencia normativa, inclusive se les reconoce eficacia para la articulación posterior de las leyes, ya que constituyen una herramienta útil para garantizar e intensificar la protección legal.

Los códigos de conducta son particularmente relevantes para los Estados que han optado por una legislación ómnibus, ya que mediante ellos se logra adecuar las disposiciones generales de la ley al contexto específico en el cual tienen lugar las operaciones de tratamiento. Por supuesto, ello es sin perjuicio de la dictación de leyes especiales, o el uso de facultades reglamentarias por la autoridad pública. Es el caso de la Unión Europea, en cuya Directiva se incluye un tratamiento específico sobre los códigos de conducta.[7]

Sin embargo, el progresivo reconocimiento obtenido por los códigos de conducta ha supuesto superar ciertos reparos inicialmente asociados a ellos y que dicen relación con la legitimidad en su proceso de elaboración, la fuerza obligatoria y la publicidad de los mismos.

El primer inconveniente relacionado con los códigos de conducta se vincula con la *representatividad* que debe suponer su proceso de elaboración, más aún cuando su eficacia radica en su voluntaria aceptación. Además, la ausencia de tal requisito puede conducir a una proliferación normativa que menoscaba toda pretensión de seguridad jurídica.[8]

En este sentido, la legislación española prescinde de la representatividad en la elaboración de códigos de conducta, admitiendo códigos individuales.[9] En cambio, la legislación de Argentina exige que su formulación sea realizada por asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada; sin embargo, no precisa las condiciones que supone tal representatividad, ni faculta a la autoridad de control para cerciorarse de ella.

Por su parte, en Reino Unido se acentúa el carácter participativo de la elaboración de los códigos, imponiendo a la autoridad de control considerar los intereses de las entidades que tratan datos, así como de las personas concernidas en ellos y los representantes de unos y otros, ya sea en las consultas que deben preceder a su aprobación o en su elaboración, según los casos. Mientras, en Italia, la ley pone de cargo de la autoridad pública velar por la observancia del principio de representatividad en la elaboración de códigos de buena conducta.

Un segundo inconveniente adjudicado a los códigos de conducta es el relativo a su *legalidad*, esto importa juzgar la adecuación de sus normas con las disposiciones legales aplicables en la materia.

La Directiva 96/45/CE se hace cargo del tema relativo a la conformidad de los códigos de conducta con las disposiciones de derecho interno o comunitario, estableciendo mecanismos para que sean sometidos al examen de las autoridades nacionales o comunitarias, las que velarán, entre otras cosas, por la conformidad normativa de los proyectos que le sean sometidos.

En el caso del Reino Unido, los códigos de conducta son sometidos a revisión del Comisionado para la Protección de Datos. Mientras, en Italia, la ley impone a la autoridad de control nacional velar por la conformidad de los códigos con las leyes y reglamentos habidos en la materia. Más expresivas todavía son las legislaciones de España y de Argentina, que facultan a la autoridad pública para dene-

---

[7] Directiva 95/46/CE del Parlamento Europeo y el Consejo de 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.

[8] En similar sentido, Puccinelli, Oscar, *Protección de datos de carácter personal*, Ed. Astrea, Bs. Aires (2004), pp. 452, 453 y 456.

[9] Parte de la doctrina rechaza la admisión de códigos de conducta de una empresa. Cf. Orti Vallejo, Antonio, *op. cit.*, p. 93; en contrario, Lucas Murillo de la Cueva, Pablo Lucas, "Informática y Protección de Datos Personales", en *Cuadernos y Debates,* Nº43, Centro de Estudios Constitucionales. Madrid (1993), p. 115, infra. 147; y, Herrán Ortíz, Ana Isabel, *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, Dykinson, Madrid (2002), pp. 311 – 315. Como quiera, diversas empresas han obtenido el registro de códigos de conducta singulares ante la autoridad de control española.

gar la inscripción del código cuando no se ajusta a las disposiciones legales o reglamentarias, permitiendo requerir de los solicitantes que efectúen las correcciones oportunas, a fin de subsanar las irregularidades.

El tercer punto que merece reparos respecto de los códigos de conducta es el relativo a la *obligatoriedad* de los mismos, lo cual supone responder a cuán vinculantes resultan sus disposiciones para sus destinatarios.[10]

La doctrina estima que el carácter voluntario de los códigos no garantiza derechos legales a ninguna de las partes intervinientes, salvo que su texto haya sido incorporado contractualmente.[11] Se han dejado sentir voces que les atribuyen el carácter de *lex artis*.[12] Hay también quienes estiman que los propios códigos debían de contemplar sanciones –de naturaleza reparadora y punitiva– que asegurasen su eficacia.[13] Para otros los códigos tienen el valor de recomendaciones y como tales la sanción que llevan aparejada es, como más, la expulsión o separación del infractor de la agrupación a que corresponde el código vulnerado.[14]

La legislación, en general, carece de una respuesta sobre la exigibilidad de los códigos de conducta. Una excepción la constituyen los *Safe Harbor Privacy Principles*[15], ya que la *Federal Trade Commission* admite que las normas de conducta adoptadas por las entidades estadounidenses vinculadas al Acuerdo revisten carácter obligatorio para las mismas, y su infracción puede dar lugar a responsabilidad, pero sólo en la medida que tales actos o prácticas constituyan actos desleales o fraudulentos en el comercio o relacionados con él.

Un cuarto aspecto que merece ser resuelto, en aras de un conveniente régimen jurídico de los códigos de conducta, es el relativo a la *publicidad* de los mismos. Si alguna eficacia normativa tienen los códigos, morigerada siquiera, ella supone la adecuada difusión de sus disposiciones, tanto entre sus destinatarios, como entre las personas concernidas por los datos, que son quienes mayor preocupación habían de revelar por el cumplimiento de sus preceptos.

En el caso de Reino Unido e Italia, la ley faculta a la autoridad pública para disponer la difusión de los códigos de conducta, sin precisar el medio por el cual se asegurará que su contenido llegue a conocimiento público. Sin embargo, la actitud más generalizada al respecto es disponer que ellos sean

---

[10] El problema concernienre a la obligatoriedad de las disposiciones adoptadas por la entidad responsable de tratamiento de datos a través de los códigos de conducta era visualizado ya en el *Lindop Report*, el que proponía que una vez aprobados gozaran del valor de disposición reglamentaria, parecer que no fue hecho propio por el legislador británico. Cf. Heredero Higueras, Manuel, *La Directiva Comunitaria de Protección de Datos de Carácter Personal*, Ed. Aranzadi, Pamplona (1997), p. 196. Para una revisión sobre las diversas opciones consideradas en el *Lindop Report* a efectos de que los códigos de conducta gozarán de obligatoriedad, cf. Losano, Mario, "Los orígenes del 'Data Protection Act' inglesa de 1984", en *Cuadernos y Debates*, N° 21, Centro de Estudios Constitucionales, Madrid, (1989). 21, pp. 9 – 60.

[11] ESTADELLA Yuste, Olga, *La protección de la Intimidad frente a la Transmisión Internacional de Datos Personales*, Ed. Tecnos, Madrid (1995), p. 44.

[12] ORTI Vallejo, Antonio, *op. cit.*, p. 93 – 94.

[13] HERRÁN Ortíz, Ana Isabel, *op. cit.*, p. 314.

[14] VELÁZQUEZ Bautista, Rafael, *Protección Jurídica de Datos Personales Automatizados*, Ed. Colex. Madrid (1993), p. 191. Este es el criterio subyacente en la regulación de los códigos de conducta en Argentina, en que la Dirección Nacional de Protección de Datos Personales debe cerciorarse de su eficacia ejecutiva con relación a los operadores del sector mediante la previsión de sanciones o mecanismos adecuados.

[15] A mediados del 2000, la Federal Trade Comission de Estados Unidos publicó los denominados *Safe Harbor Privacy Principles*, traducidos como Principios de Puerto Seguro, texto que contempla los principios a que deben sujetarse las entidades estadounidenses para obtener el visto bueno de la Unión Europea, a fin de asegurar una política de protección de datos adecuada, que brinden privacidad y confidencialidad homologables a los estándares europeos, tras lo cual podrán recibir cesiones de datos personales provenientes de los Estados miembros de la Unión Europea sin problemas ni sanciones para cedente o cesionario. Vid. Cerda, Alberto, "Autodeterminación Informativa y Leyes sobre Protección de Datos", en *Revista Chilena de Derecho Informático*, núm. 3 (2003), pp. 47 – 75.

inscritos en el registro que lleva al efecto la autoridad de control respectiva. Es la fórmula adoptada en Argentina y en España. En similar sentido se pronuncia *Safe Harbor Privacy Principles*, respecto de los códigos adoptados por las entidades adherentes al Acuerdo, los que deben ser registrados por la *Federal Trade Commission.*

La apretada descripción de los códigos de conducta, así como sus ventajas y en especial las desventajas atribuidas a los mismos, permite apreciar que su incorporación en el sistema diseñado por las leyes sobre protección de datos se conjuga con la existencia de una autoridad de control, que fomenta su elaboración, vela por la representatividad y legalidad de los mismos, les brinda difusión y, en ciertos casos, fiscaliza la adecuación de las operaciones al mismo.

4.- Mecanismos de autocontrol: agente de control interno

La primera legislación sobre tratamiento de datos se caracterizaba por establecer férreos controles por parte de la autoridad pública al procesamiento de datos. Una política de control tan estricta tenía sentido en cuanto el equipamiento informático era escaso y el desarrollo de la telemática incipiente; sin embargo, el exponencial desarrollo de la computación, asociado al potencial de las telecomunicaciones había de revertir las pretensiones de un control público centralizado, haciendo necesaria la adopción de mecanismos de control que, conjugados con una autoridad, hiciere más eficaz los propósitos de la legislación.

En este sentido, la proliferación de los sistemas de tratamiento y la propagación de los datos personales, particularmente por entidades del sector privado, hacía necesaria la implementación de un mecanismo de control que no descansara exclusivamente en una fiscalización "virtual", remota si se prefiere, sino que guardara más cercanía con las operaciones cotidianas de tratamiento: un agente de control interno.

La figura se prevé por la Directiva 95/46/CE con el nombre de *encargado de tratamiento*, quien es nombrado por el responsable del tratamiento para cerciorarse de que las operaciones efectuadas no atentan contra los derechos y libertades de los interesados.[16] En el derecho comparado este instituto presenta cuatro características comunes:

i. El agente de control interno es un *tercero*, esto es, se trata de una persona distinta del responsable de tratamiento.[17]
ii. El agente de control interno es un *técnico,* vale decir, posee la competencia profesional y la fiabilidad necesaria para poder cumplir sus funciones.
iii. El agente de control interno es designado por el responsable de tratamiento. Precisamente, la circunstancia de ser nombrado por quien detenta las facultades para adoptar decisiones respecto de las operaciones que recaen sobre los datos permite calificar al agente de control interno como un mecanismo de autocontrol.
iv. El agente de control interno debe ejercer sus funciones con total *independencia.* Una de las cualidades unánimemente adjudicadas al agente de control interno, aun tratándose de aquél sujeto a dependencia laboral de la entidad responsable de tratamiento de datos respecto de la

[16] Sobre la incorporación de la figura por la Directiva 95/46/CE, Cf. HEREDERO Higueras, Manuel, *La Directiva Comunitaria..., op. cit.*, pp. 169 – 170. Sobre la inspección administrativa mediante sujetos privados, en que el agente de control interno es denominado *colaborador*, Cf. Rivero Ortega, Ricardo, *El Estado vigilante. Consideraciones jurídicas sobre la función inspectora de la administración,* Ed. Tecnos, Madrid (2000), pp. 149 y ss.

[17] Jurídicamente, el agente de control interno no constituye un tercero, y alguna legislación se encarga de puntualizar tal circunstancia (así sucede con la Directiva 95/46/CE y con la Ley de Datos de Suecia), con el propósito de hacer extensivas a su respecto las obligaciones que se imponen al responsable de la base de datos, así como a quienes procesan tales datos por encargo de éste, particularmente por lo tocante a la confidencialidad y seguridad.

cual ejerce sus labores fiscalizadoras, es la plena independencia con la cual debe desempeñar su cometido.

La figura del agente de control interno puede ser asociada al tratamiento de datos personales efectuados tanto en el sector público como en el privado. Así se prevé en la Directiva de la Unión Europea e igualmente en las legislaciones de Inglaterra y Suecia. En cambio, en la legislación alemana su ámbito de aplicación se circunscribe a personas o entidades privadas.

La principal ventaja atribuida al agente de control interno, en cuanto mecanismo de control, radica en la continuidad y proximidad de su cometido en relación con las operaciones efectuadas por la entidad responsable de tratamiento. Además, el agente de control interno orienta y asiste a la empresa y a las personas empleadas en el procesamiento de datos, acerca del modo de proceder en la materia, mediatiza la relación entre las personas afectadas por el tratamiento de datos y la entidad a la cual controla y vincula a ésta con la autoridad pública de control.

Pese a la utilidad que significa disponer de un mecanismo de control como el que se viene comentando, la institución del agente de control interno no ha estado exenta de críticas; éstas se han centrado en que su establecimiento menoscabaría la protección de los titulares de datos, al dejar el control sobre la legalidad de su tratamiento entregado a un tercero empleado del propio responsable de la base de datos, con una independencia meramente formal que no satisface las exigencias de un efectivo control.

No obstante, nos parece que el reparo formulado contra el agente de control interno evidencia una insuficiente documentación en quienes le sostienen, ya que supone que el control se radica en forma exclusiva y excluyente en tal figura, cuando la experiencia de derecho comparado demuestra que la institución conjuga su quehacer con el accionar de la autoridad pública de control, además de no obstar al ejercicio de las facultades que la ley asigna a ésta, así como a los propios titulares de los datos personales.

5.- Modelo integrado de regulación y control

Ya antes hemos dejado establecido que los distintos países que han reglamentado el tratamiento de los datos personales disponen de leyes más o menos específicas sobre la materia, así como de mecanismos de control jurisdiccional. No obstante, entre unas experiencias y otras es posible constatar diferencias: en ciertos sistemas se ha creído necesario establecer un organismo público independiente que vela por el cumplimiento de la ley, disponiendo de facultades normativas y fiscalizadoras; en cambio, en otros sistemas se prescinde de una autoridad similar, alentándose a los propios interesados para la adopción de patrones de conducta y mecanismos de control.

En ocasiones, un organismo como el antes mencionado ha desplazado el rol de los propios actores relevantes en la regulación y control, tal ha sido el caso de la primera experiencia legislativa de Suecia. En otros, tal organismo no existe o carece de facultades suficientes, es el caso de Estados Unidos y de Chile. Es también el estándar alentado por APEC Privacy Framework.

Sin embargo, como hemos podido apreciar de la breve reseña en cuanto a los códigos de conducta y al agente de control interno, las opciones no son químicamente puras, y más bien se observa un tramado de opciones de autorregulación y autocontrol que se conjugan con una autoridad pública que detenta facultades normativas y fiscalizadoras, entre otras. Es lo que observa en los países que integran la Unión Europea, pero también es cuanto se aprecia en otras latitudes, así en Argentina, Australia, Canadá y Hong-Kong, por mencionar algunas.

La considerable distancia que media entre las disposiciones legales y la solución jurisdiccional obsta a la obtención de un adecuado nivel de protección para los derechos de las personas concernidas

por los datos personales. Sin embargo, tal trecho puede ser salvado parcialmente mediante el expediente de recurrir a mecanismos de autorregulación y autocontrol, tales como los códigos de conducta y el agente de control interno, por mencionar algunos. Pero no puede obviarse que estos mecanismos resultan fatuos e insuficientes si no se adoptan medidas apropiadas para garantizar su utilidad. Es precisamente en este punto donde resulta del todo necesario disponer de una autoridad pública que garantice la observancia de la ley.

Conclusiones

Un adecuado nivel de protección se obtiene de la conjugación de mecanismos de autocontrol que se traslapan con la institución de una autoridad de control que, en cuanto elemento esencial del sistema, vela por el cumplimiento de la normativa sobre tratamiento de datos. Se trata de una institucionalidad que media entre las generales disposiciones de la ley y los particulares efectos de las resoluciones judiciales. Es lo que hemos denominado un modelo integrado de protección, es el modelo hacia el cual progresivamente se converge, con mayor o menor énfasis, y desde distintas latitudes.[18]

Así pues, reconociendo lo razonable que resulta atribuir a los propios agentes sociales involucrados responsabilidad en la regulación y resolución de los conflictos originados del incumplimiento de la normativa sobre tratamiento de datos personales -la autorregulación y el autocontrol contribuyen a construir un nivel de protección adecuado-, sin una autoridad pública de control resultan una ilusión, una quimera, un puro artificio y, en determinados casos, una verdadera pesadilla.

La construcción de un sistema de protección eficaz para garantizar los derechos fundamentales comprometidos y, a la vez, evitar que los desequilibrios normativos entorpezcan el adecuado funcionamiento de los mercados, supone la conjugación de los mecanismos de autorregulación y autocontrol con la acción de una autoridad pública que garantice el cumplimiento de la ley.

El avance de la tecnología contribuye a mejorar la calidad de vida, pero, a la vez, crea nuevos riesgos y conjurarlos no es sólo una labor individual de las personas, sino también un cometido de nuestros Estados.

Bibliografía

CERDA, Alberto, "La autoridad de control sobre protección de datos personales", en Anales de la Facultad de Derecho, Santiago, Universidad de Chile, núm. 2, 2005.

ESTADELLA Yuste, Olga, *La protección de la Intimidad frente a la Transmisión Internacional de Datos Personales*, Ed. Tecnos, Madrid, 1995.

HEREDERO Higueras, Manuel, *La Directiva Comunitaria de Protección de Datos de Carácter Personal*, Ed. Aranzadi, Pamplona, 1997.

HERRÁN Ortíz, Ana Isabel, *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, Dykinson, Madrid, 2002.

[18] David Loukidelis, Information & Privacy Commissioner for British Columbia (Canadá), alude a sistemas mixtos o híbridos, en los cuales se conjugan experiencias de regulación y control estatal, con normas y prácticas de control adoptadas por los propios actores sociales relevados, en especial entidades responsables de tratamiento de datos. Vid. LOUKIDELIS, David, *"An Overview of Information Privacy"*, APEC Symposium on Information Privacy in E-Government & E-Commerce, Ha Noi, Vietnam, February 22, 2006.

LOUKIDELIS, David, *"An Overview of Information Privacy"*, APEC Symposium on Information Privacy in E-Government & E-Commerce, Ha Noi, Vietnam, February 22, 2006.

MURILLO de la Cueva, Pablo Lucas, "Informática y Protección de Datos Personales", en Cuadernos y Debates, N°43, Centro de Estudios Constitucionales. Madrid.

ORTI Vallejo, Antonio, *Derecho a la intimidad e informática*, Ed. Comares, España, 1994.

Puccinelli, Oscar, *Protección de datos de carácter personal*, Ed. Astrea, Bs. Aires, 2004.

SHAPIRO, Andrew, *The control revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know,* Public Affairs/The Century Foundation, 1a. ed. en ingles, 1999, *El mundo en un clic,* trad. Francisco Ramos, Grijalbo. Barcelona, 2001.

VELÁZQUEZ Bautista, Rafael, *Protección Jurídica de Datos Personales Automatizados,* Ed. Colex. Madrid, 1993.