INFORMATICA Y LIBERTAD: LA RESPUESTA DE LOS JURISTAS A UN PROBLEMA DE NUESTRO TIEMPO

Por MANUEL HEREDERO HIGUERAS

Sumario: 1. INTRODUCCIÓN: LA CRECIENTE INQUIETUD POR LA PÉRDIDA DEL CONTROL DE LA INFORMÁTICA.—2. ASPECTOS DEL PROBLEMA: 2.1. Aspecto tecnológico. 2.2. Aspecto deontológico. 2.3. Aspecto jurídico.—3. EL ASPECTO JURÍDICO Y SUS SOLUCIONES: 3.1. El movimiento legislativo. 3.2. El movimiento doctrinal.—4. EL PROBLEMA EN ESPAÑA. APÉNDICE DOCUMENTAL: 1. Ley de Protección de Datos, promulgada el 7 de octubre de 1970, por el Ministro Presidente del Estado de Hesse (Alemania Federal). 2. Ley (sueca) de Protección de Datos (*datalag*, SFS 1973: 289). Ley de privacidad, de 1974 (EE. UU.).

1. Introducción: la creciente inquietud por la pérdida del control de la informática

En las últimas décadas hemos asistido al desarrollo incontrolado de diversos fenómenos tecnológicos, tales como la astronáutica, la energía nuclear, la televisión, el automóvil, la informática. Todos estos fenómenos han ido creando una serie de consecuencias inesperadas que han surgido, aparentemente, por sorpresa. La gravedad de este proceso ha hecho surgir una creciente preocupación por las consecuencias imprevisibles que pudieran derivarse de la propia dinámica interna de estas tecnologías, aisladas o unidas. En el caso de la informática, o más exactamente, del uso generalizado de los ordenadores, esta pre-

ocupación obedece a causas diversas. En primer lugar, el individuo teme perder todo control de sus datos personales. Este temor se debe, ante todo, a la *vulnerabilidad de la información*. La introducción de información en el ordenador exige unos procesos de elaboración intermedia, como la codificación y transcripción, que por sí mismos crean un riesgo de intrusión. Por otra parte, los soportes en que se graba o transcribe la información son muy reducidos en proporción a la cantidad de información que pueden contener; por ello, el robo de una cinta magnética permite acceder a una cantidad de datos que en forma descodificada podrían ocupar una cierta cantidad de papel o material análogo. Este hecho hace posible el espionaje industrial en gran escala, por ejemplo. También es posible que la cinta contenga un programa complejo, lo cual podría impedir el funcionamiento del sistema correspondiente o permitiría sabotajes de los servicios o actividades a que el sistema estuviere afectado. Esta vulnerabilidad se manifiesta igualmente en la mayor facilidad con que los soportes informatizados pueden ser destruidos o borrados, no ya por accidentes, sino por medios específicamente aptos (un simple imán puede borrar toda la información contenida en un carrete de cinta). Esta facilidad contrasta con la dificultad que implica la destrucción de documentación ordinaria (que exige máquinas especiales).

La vulnerabilidad no se limita a la información, sino que afecta al propio *tratamiento de los datos*. Un grano de polvo o una variación de escasa importancia del suministro de la corriente eléctrica pueden hacer que los datos se pierdan o transformen o sean transferidos a campos o a dispositivos distintos de los previstos. Según estudios de un suministrador, en las transmisiones de datos por canales de voz, a velocidades de 600 y 1.200 bitios por segundo, la frecuencia de la producción de errores se dobla cuando se dobla la velocidad de transmisión, y aumenta en general al aumentar la distancia. Además de estos factores de difícil previsibilidad, hay otros más directamente relacionados con el factor humano, como la intercalación en un programa de instrucciones mediante las cuales se falseen intencionadamente los resultados o se obtengan resultados no previstos. En un programa de nóminas podrían lograrse

detracciones considerables de dinero a favor de uno de los interesados con ayuda de un adecuado juego de instrucciones.

Aparte de esta vulnerabilidad de la información, la pérdida del control de la misma por el interesado se debe a las dificultades que para el individuo ofrece la comprensión del alcance de cada dato concreto de los que componen el registro informatizado de una persona. A veces la petición de determinados datos puede tener como finalidad la cancelación de datos que pueden tener efectos negativos (anotaciones policiales, que pueden quedar anuladas con simples actualizaciones de registro). La forma críptica en que se registran los datos, incluso en los formularios de captación de datos, se presta a interpretaciones diversas. Del mismo modo que el niño que se extravía en la niebla o en la noche, el individuo que sabe que está registrado en un conjunto de ficheros que no ve ni conoce, tiende a exagerar y a añadir a los peligros reales riesgos imaginarios. Esta dificultad de interpretación impide a veces la cancelación de datos obsoletos. Llevadas al extremo las consecuencias de este hecho, pueden originarse verdaderas «cárceles informatizadas» en cuanto que las personas a quienes afectan los datos obsoletos, pero desfavorables, pueden verse privadas de oportunidades profesionales o estar afectadas permanentemente de juicios negativos en el orden humano, político, religioso, etc.

Otra causa de inquietud estriba en los peligros que la informatización ofrece como instrumento de vigilancia y control del individuo. Un caso extremo lo constituye el uso de ciertas técnicas informáticas basadas en dispositivos de exploración de documentos. Mediante estos dispositivos la Administración Postal norteamericana registra de cada sobre el destinatario, el remitente, la fecha y lugar del franqueo, la clase de envío, sin necesidad de abrir la carta ni de demorarla. El ordenador provisto de explorador recoge esta información automáticamente y después puede ponerla en relación con otra análoga y establecer conclusiones acerca de las relaciones postales de una persona con otras. Así puede anotarse en una ficha policial que «X sostiene correspondencia con Y, agente comunista», por ejemplo. Esta información no puede ser utilizada como prueba en un proceso, pero sí como guía orientadora de una investigación.

El problema se plantearía si una empresa privada, sobre todo de las dedicadas a asesorar sobre la solvencia, se sirviere de estos dispositivos para valorar a sus clientes. A partir de esta información cabe también construir modelos de comportamiento de las empresas y predecir sus reacciones ante determinadas campañas de producción o de venta. Si a todo esto se añaden las posibilidades que actualmente ofrecen los sistemas de toma de datos a distancia (satélites, aviones de gran altura), los cuales hacen posible identificar bancos de peces en el océano y seguir sus movimientos, así como las plantaciones de drogas, etc., se comprenderá que tal inquietud tiene un sólido fundamento.

No toda la información ni todo tratamiento de la información ofrece el mismo grado de vulnerabilidad. Tampoco ésta se manifiesta en igual forma en el ámbito privado y en el público. Asimismo, la circulación de la información presenta problemas diversos según que se limite al interior de los Estados o que trascienda del ámbito de las fronteras nacionales.

Sin duda alguna, la información referente a cosas aisladamente consideradas no suscita problema alguno, en principio. Antes, al contrario, su difusión, su libre circulación, deben fomentarse, con la sola reserva de las necesidades estratégicas o de la defensa o la seguridad nacional. Muy distinto es el caso de que una información acerca de una cosa (un vehículo, una vivienda) pueda ser puesta en relación con una persona: la propiedad de un vehículo por una persona añade algo a los datos estrictamente personales; lo mismo sucede con la propiedad de un barco, de una aeronave o una explotación agraria. Esta información determina la aparición de supuestos de hecho que, a su vez, llevan aparejadas consecuencias jurídicas en el ámbito civil, mercantil, fiscal, etc.

Por otra parte, si bien es la informatización de los archivos o ficheros lo que determina esa vulnerabilidad especial, no es menos cierto que los ficheros manuales, o no automáticos, ofrecen igualmente ciertos riesgos. Sin duda, ha sido una consecuencia indirecta del planteamiento de esta problemática informática la conciencia de una vulnerabilidad de los ficheros manuales. Pero en este supuesto, los problemas se manifiestan en un plano diferente: la vulnerabilidad no es consecuencia de la inestabi-

lidad de los soportes físicos ni de la instantaneidad del acceso a los datos, sino de la posibilidad de un tráfico indebido de la información (venta o cesión de listas de miembros de una asociación, de una lista de electores), o de la ignorancia de los datos por parte del interesado, o del uso inadecuado de la información (utilización de las listas de abonados al teléfono como colectivos a efectos de estudios de prospección de mercados, etcétera). La problemática suscitada por la informatización ha descubierto la existencia de zonas conflictivas comunes a los ficheros automáticos y a los manuales.

Finalmente, la circulación de la información no ofrece igual fisonomía en el seno de un Estado y en la comunidad internacional. En este segundo supuesto surgen problemas que inciden en la soberanía de los Estados: la información (objetiva o personal, sin distinción en este caso) es parte del ámbito material de soberanía, que no se limita al territorio en sus diversas formas. La soberanía de la información viene impuesta por la sola mecánica del Estado como organización; como tal, necesita disponer de la información precisa para adoptar las decisiones que sus fines institucionales exigen en cada momento.

2. Aspectos del problema

2.1. Aspecto tecnológico

Si bien esta preocupación puede no ser del todo fundada, los profesionales de la informática, los juristas y diversos otros profesionales han ido estudiando la posibilidad de arbitrar unas medidas de índole diversa que permitan hacer frente a los peligros, reales o imaginarios, del uso generalizado de los ordenadores. A tal efecto, se distinguen tres órdenes de problemas: un problema de carácter *tecnológico*, consistente en cómo impedir el acceso incontrolado a los sistemas de proceso de datos mediante la concepción y realización de unos dispositivos físicos o lógicos que lo impidan; un problema *deontológico* que exige la creación de una mentalidad responsable por parte de los profesionales y la aceptación de unos códigos de ética informática;

y, finalmente, un problema estrictamente *jurídico*, el de crear un marco conceptual que permita sistematizar los supuestos de hecho posibles y darles una solución coherente y uniforme.

El primer problema ha sido objeto de atención por parte de los suministradores. Se han diseñado dispositivos específicos que hacen referencia al control del acceso a los sistemas, en forma de conmutadores separados para el suministro de la energía, dispositivos de identificación del usuario (palabras clave y tarjetas de identificación, sistemas de *voice-print)*, dispositivos de comprobación de los programas (que en casos de desviaciones del proceso normal del programa producen determinadas reacciones).

2.2. Aspecto deontológico

La imposibilidad de lograr un control o vigilancia de los distintos actos profesionales del informático ha llevado a pensar que la mejor garantía contra el uso abusivo del ordenador consiste en una ética profesional sólida. La mayor parte de los profesionales de la informática son todavía jóvenes, cambian con frecuencia de empleo y carecen de las tradiciones que en punto a ética profesional poseen la profesión médica o la jurídica, por ejemplo. Por ello, se han hecho diversos intentos para redactar códigos de deontología informática, entre los cuales deben mencionarse los de la Association for Computing Machinery y de la British Computer Society (1).

2.3. Aspecto jurídico

Las medidas de índole tecnológica y deontológica no son suficientes. Es preciso además elaborar unos principios o reglas de Derecho objetivo que puedan ser aplicados a los supuestos de hecho que se van perfilandc y a los que vayan apareciendo. En el caso de la defensa contra el uso indebido de los ordenadores

(1) En nuestro país la fundación CITEMA encomendó a un grupo especial de trabajo la elaboración de unas «normas básicas de deontología informática», que fueron publicadas en 1974, y en cuyo apéndice figura una amplia bibliografía sobre el tema.

se han seguido dos caminos: redacción de textos legales, de una parte, y búsqueda de nuevas reglas o principios jurídicos a partir de conceptos o construcciones dogmáticas ya existentes. Asimismo, ciertos conflictos de intereses que se van dibujando exigen todavía una clarificación y unas soluciones. Todas estas opciones, a primera vista no del todo justificadas, obedecen a la preocupación de evitar que con el fenómeno informático suceda lo que ha ocurrido con otros fenómenos tecnológicos, como la contaminación del medio ambiente. En el caso de la contaminación, el legislador se ha visto cogido por sorpresa, teniendo que hacer frente a un problema ya existente y de suma gravedad. En el caso de la informática, es posible todavía crear un marco que encauce el fenómeno, de tal manera que puedan evitarse las graves consecuencias que pudieran derivarse de su desarollo incontrolado. Conviene precisar que el expresado movimiento no aspira a crear un mero mecanismo de represión del uso de los ordenadores, un freno al desarrollo de la informática, sino que más bien tiende a restablecer un equilibrio jurídico roto en cierta manera por la irrupción incontrolada del fenómeno (2).

3. El aspecto jurídico y sus evoluciones

3.1. El movimiento legislativo

El aludido movimiento legislativo está jalonado por un conjunto de Leyes y proyectos o proposiciones de Ley (una veintena) (3), que han conocido diversa suerte, ya que mientras unos han pasado ya la mayoría de los estadios del proceso legislativo, otros han quedado abandonados u obsoletos. La primera Ley de protección de datos conocida es la promulgada el 7 de octubre

(2) Sobre la distinción que los sociólogos hacen entre Derecho represivo y Derecho restitutivo, cfr. Rocher, G.: *Introduction à la sociologie générale*, 2. L'organisation sociale, París, Editions HMH, 1968.

(3) Véase una exposición sistematizada de las legislaciones nacionales existentes en la publicacion del Consejo de Europa *La protection des données en Europe*, Estrasburgo, 1975. En el Apéndice Documental del presente trabajo figura una versión española de los tres textos que se hallan en vigor: la Ley sueca, la de Hesse y la *Privacy Act*.

de 1970 en el Estado alemán occidental de Hesse. Le siguieron la Ley sueca de datos *(Datalag)*, de 1972 (4), y la Ley de privacidad *(Privacy Act)* norteamericana, de 1974 (5). Próximos a ser aprobados como leyes se hallan un proyecto alemán federal (6), un proyecto austríaco (7), un proyecto norteamericano federal referido específicamente a la información judicial penal (8), dos proyectos noruegos, relativos al uso de los sistemas de datos personales creados por órganos del Estado o del Municipio (9) y al tratamiento de la información por entes privados (10), así como el proyecto danés de Ley de registros privados (11) y, el más reciente, un proyecto francés que acaba de ser sometido por el Gobierno a la Asamblea Nacional (12). Podemos considerar como abandonadas las proposiciones de ley británicas denominadas *Data Surveillance Bill* (13) *y Bill on Personal Information* (14), así como la proposición de Ley francesa, presenta-

(4) SFS 1973: 289.

(5) Public law 93-579, 93rd Congress, S. 3418. También se dispone de legislación específica sobre la materia en Alaska, California, Iowa y Massachusetts. Véase el Apéndice Documental citado en la nota 3.

(6) Deutscher Bundestag, Drucksache 7/1027.

(7) Número 1423 de Beilagen zu den stenographischen Protokollen des Nationalrates, XIII GP.

(8) S. 2008 (1975).

(9) NOU 1975: 10.

(10) NOU 1974: 22.

(11) Betaenkning nr. 687, 1973.

(12) Proyecto de ley relativo a la informática y a las libertades, presentado a la Asamblea Nacional por J. Lecanuet en nombre del primer ministro J. Chirac (Assemblée Nationale, Quinta legislatura de la Constitución de 1958, núm. 2516; primera sesión ordinaria de 1976-77).

(13) Proposición de ley elevada a la Cámara de los Comunes por KENNETH BAKER el 6 de mayo de 1969, y a la de los Lores por lord WINDLESHAM el 26 de junio de 1969. En la Cámara de los Comunes no pasó la segunda lectura; en la de los Lores fue objeto de debate el 3 de diciembre de 1969, sin que se entrara en el fondo del problema ni se llegara a conclusión alguna. Cfr. WARNER-STONE: *The Data Bank Society*, Londres, Allen & Unwin, 1970.

(14) Proposición de ley redactada por el National Council for Civil Liberties (NCCL) de Gran Bretaña. El texto se recoge en la publicación Privacy, *Computers and You*, editada en 1972 conjuntamente por el National Computing Centre Ltd. de Manchester y el NCCL, y que contiene las deliberaciones y ponencias de un seminario celebrado en Londres los días 18 y 19 de noviembre de 1970, convocado por el NCCL y la editorial Allen & Unwin.

Con posterioridad a estas dos proposiciones de Ley se han realizado estudios que han llevado a la conclusión de la conveniencia de una legislación sobre el tema. Fruto de una primera comisión de estudios fue el informe Younger (1972), referido solamente a los ficheros privados. Abundando en ideas de dicho informe, fue publicado en diciembre de 1975 el Libro Blanco titulado *Computers and Privacy* (Cmnd. 6353). Para redactar el proyecto de Ley propugnado por el Libro Blanco se creó una comisión especializada, denominada *Data Protection Committee*. Se espera que esta comisión necesite unos dos años para ultimar su labor.

da por el entonces diputado Poniatowski, por la que se pretendía crear un Tribunal de la Informática (15).

Paralelamente, se han ido aprobando proyectos de ley que hacen referencia a la protección de datos en ámbitos más específicos. Es el caso de la Ley norteamericana de evaluación leal de la solvencia *(Fair credit Reporting Act)* (16), de la Ley sueca de información crediticia (17), y de la Ley sueca de cobros privados *(Inkassolag)* (18).

En realidad, estos otros textos hacen referencia a actividades no específicamente informáticas, pero que, como consecuencia del planteamiento de la problemática de la protección de datos, han mostrado una cierta semejanza con la informática en cuanto a su vulnerabilidad. Es el caso de actividades tales como la valoración de la solvencia, las encuestas de opinión, la venta de listas de personas con fines de encuesta o de otro tipo, etc.

3.2. El movimiento doctrinal

3.2.1 *La teoría del «derecho de privacidad»*

3.2.1.1 Paralelamente al movimiento legislativo, y a la vez como parte del mismo o como punto de partida, se han recogido conceptos jurídicos ya formulados, ampliando su ámbito de aplicación, o bien se han creado o formulado conceptos nuevos. Entre los primeros, el más extendido —al menos, en un primer momento— es el llamado «derecho de privacidad» *(right of privacy)*. Este concepto fue elaborado en los últimos años del siglo pasado por dos juristas norteamericanos, Warren y Bran-

(15) Proposición de Ley presentada por M. Poniatowski y el grupo de diputados republicanos independientes y coaligados el 30 de octubre de 1970, a la Asamblea Nacional de Francia. Preveía la creación de un Comité de Vigilancia y un Tribunal de la Informática, aduciendo como fundamento peligros diversos de los ordenadores, entre ellos la posibilidad de que un día llegaren a ser inteligentes («La machine risque de devenir intelligente»). El senador H. Caillavet recogió el mismo texto, sin más alteración que la de sustituir el Comité de Vigilancia por un Directorio, y presentó una proposición de Ley análoga ante el Senado francés en la sesión de 1973-74.

(16) Aprobada en 1970 como título VI de la Ley de Protección al Consumidor. Revisada en noviembre de 1973.

(17) SFS 1973: 1173.

(18) SFS 1974: 327.

DEIS (19), con el fin de hacer frente al problema de la progresiva invasión de la intimidad por los medios de información. El derecho a la intimidad se definió como «derecho a ser dejado a solas» *(right to be let alone)*. Las nuevas dimensiones aportadas al problema de la defensa de la intimidad por la difusión del uso de los ordenadores obligó a una reformulación del concepto. La fórmula más extendida para redefinirlo es la siguiente: «El derecho del individuo a decidir por sí mismo en qué medida quiere compartir con otros sus pensamientos y sentimientos, así como los hechos de su vida personal» (20).

Esta definición pretende dar una nueva configuración al concepto formulado por WARREN y BRANDEIS en 1890. Sin embargo, los juristas norteamericanos que han tratado el tema lo que han pretendido es encuadrar los nuevos supuestos de hecho en el marco de la estructura que la jurisprudencia norteamericana ha ido dando al concepto acuñado en 1890. El resultado de la elaboración jurisprudencial ha sido un concepto sumamente fluido y heterogéneo.

No obstante la fluidez de dicho concepto (21), los tratadistas han distinguido cuatro grandes facetas o aspectos, correspondientes a otros tantos supuestos de hecho: *a)* apropiación del nombre o imagen de otra persona en provecho propio: *b)* intrusión en la intimidad o en los asuntos privados de una persona;

---

(19) La primera —y clásica— construcción del concepto de *right of privacy* se encuentra en el conocido trabajo de WARREN y BRANDEIS: «The right to privacy», publicado en la *Harvard Law Review*, vol. 4 (1890). Con posterioridad han sido frecuentes las recapitulaciones y exposiciones de la progresiva elaboración jurisprudencial del concepto. Cfr., en especial, NIZER, L.: «The right of privacy. A half century's development», *Michigan Law Review*, vol. 39 (1941); FEINBERG, W., «Recent developments in the law of privacy», *Columbia Law Review*, vol. 20 (1948).

(20) Esta definición aparece en el informe titulado *Privacy and Behavioral Research*, Office of Science and Technology, Executive Office of the President, Washington D. C., 1967. Asimismo, cfr. WESTIN, A.: *Hearings before the Subcommittee on Administrative Practice and Procedure of the Committee of the Judiciary*, U. S. Senate, 90th Congress, First Session, 1967; MUTZ, G.: «Rechtsprobleme des sogenannten Datenschutzes», *Juristische Blätter*, año 95, núms. 9/10.

(21) El concepto del *right of privacy* ha sido comparado a un «almiar en medio de un huracán» *(haystack in a hurricane)*; dentro del mismo se comprenden conceptos jurídicos muy heterogéneos, que en los sistemas derivados del Derecho romano pertenecen a ramas diversas del Derecho (culpa extracontractual, daño moral, propiedad industrial, derecho al nombre y a la imagen, etc.). Esta variedad de supuestos ha sido sistematizada en la forma que se recoge en este trabajo por W. PROSSER en su trabajo «Privacy», *California Law Review*, vol. 48; la sistematización de Prosser se utiliza asimismo como criterio expositivo en MILLER, A. R.: *The assault on privacy*. Signet Books, 1972, capítulo V-2.

c) revelación pública de hechos privados enojosos relativos a una persona; *d)* publicidad capaz de colocar a una persona bajo una falsa luz ante los ojos del público. Esta clasificación se considera como la más válida y es, asimismo, la que tienden a aceptar los jueces.

MILLER (22) estima que estas cuatro facetas del concepto son plenamente válidas como remedios jurídicos enderezados a reprimir el abuso de la información computadorizada e indirectamente a disuadir de tal abuso.

Por lo que respecta a la noción de la *apropiación del nombre o imagen,* cabe afirmar que el registro que comprende los datos de una persona grabados o perforados en dispositivos accesibles por ordenador puede contener un «retrato» de dicha persona tan completo como una fotografía. Sin embargo, aparte de las diferencias existentes entre una fotografía y un registro de memoria de ordenador, la jurisprudencia presenta ciertas dificultades, ya que la analogía exigiría dos condiciones: apropiación de la totalidad de la «imagen» informatizada y veracidad de tal imagen (lo cual dejaría fuera de la protección de la acción de privacidad a los supuestos de facilitación de datos erróneos). El estudio detenido de las sentencias que definen esta faceta de la «apreciación» muestra, no obstante, que lo que los Tribunales pretenden prevenir o reprimir es la utilización comercial de la información personal. Sería preciso que los jueces insistieran en este aspecto y pusieran menos énfasis en la idea de la apropiación del nombre o imagen, para que la noción de la apropiación pudiera jugar plenamente como remedio contra el uso indebido del ordenador. Tal orientación de la jurisprudencia facilitaría una base racional para limitar la apropiación o la venta de registros computadorizados y permitiría resolver un buen número de problemas de protección de la información, tales como los suscitados por las oficinas de crédito y las ventas de listas postales.

Más difícil resulta adaptar al contexto informático la categoría de la *intrusión,* ya que el uso indebido de la información registrada en memoria no implica una invasión directa o física. Por otra parte, la intrusión como tal define la conducta que cons-

(22) MILLER, A. R.: *Ibid.*

tituye la violación de la intimidad, pero no hace referencia a lo que a continuación se haga con los frutos de la invasión. En cambio, en el contexto informático la principal amenaza contra la intimidad es el uso subsiguiente de los datos. Sin embargo, dos sentencias recientes que han creado jurisprudencia permiten ensanchar el concepto: una de ellas (el caso Dodd) dice expresamente que es válida la ampliación del ámbito del entuerto de invasión de la privacidad a los supuestos de intrusión, mediante acto físico o no, en esferas de las cuales el ciudadano ordinario pueda razonablemente esperar que deban ser excluidos los particulares. La otra sentencia es la recaída en el célebre caso *Nader c. General Motors Corp.*, en cuyos fundamentos de hecho se contenían actividades diversas de invasión de la intimidad (intervención del telófono, pesquisas entre los amigos de Nader acerca de sus costumbres, ideas religiosas, inclinaciones sexuales, etc.); en esta sentencia también se ensanchó el concepto de intrusión en tal sentido. Cabría llevar aún más lejos este ensanchamiento del concepto e incluir en el supuesto de la intrusión toda forma de colecta de datos que implicara una indagación precisa y ofensiva de los asuntos personales de una persona. Nuevamente el caso de las oficinas de crédito podría prestarse a la acción de privacidad.

El tercero de los cuatro grandes supuestos aludidos lo constituye la revelación pública de información privada. La creación de grandes bancos de datos y el desarrollo de redes nacionales de transmisión de datos crean una potencial amenaza de que la información privada se filtre o sufra «escapes» y vaya a parar al público, amenaza que crece a medida que la evolución tecnológica permite un almacenamiento cada vez mayor de datos. El problema en este supuesto lo constituye el requisito de la publicidad de los datos obtenidos. Cabe obtener datos ajenos cuando, dentro de una explotación en tiempo compartido, se interconectan sistemas y se explotan archivos de otros usuarios. En tales casos es posible transferir datos a otros sistemas, intencionadamente y causar perjuicio al interesado sin necesidad de difundir los datos. Sin embargo, también en este supuesto la jurisprudencia ha mostrado cierta elasticidad, admitiendo excepciones al requisito de la publicidad cuando la obtención de los datos

es fruto de la violación de una relación de confianza (entre médico y enfermo, por ejemplo). Es dudoso, sin embargo, que entre el titular de un registro informatizado, que haya sido objeto de invasión de la intimidad, y el recopilador de datos no autorizado haya relación alguna de confianza. Más adecuado sería ensanchar esta noción de relación de confidencialidad o imponer un deber general de custodia a los operadores de ordenador (o tomar como punto de partida la ficción de un tal deber de custodia).

Este tercer supuesto exige además que la información hecha pública sea privada. En este punto es donde más problemática resulta la noción del «derecho de privacidad». Este punto es el que ofrece mayor dificultad. La propia doctrina norteamericana está divdida en cuanto a cuáles deban ser las «zonas de privacidad» jurídicamente protegibles. La jurisprudencia ha tratado de delimitar lo que tiene naturaleza privada frente a los casos en que existe un interés público protegible. Para ello ha tratado de hacer extensivas a la acción de privacidad las excepciones que se habían ido definiendo en las sentencias sobre calumnia y difamación. Sin embargo, la transposición de estas excepciones al contexto informático no parece viable. Una de tales excepciones, por ejemplo, es el consentimiento del ofendido. No cabría plantear en estos términos los casos en que existe un interés común entre el que difunde la información y el que la recibe, como sucede entre las organizaciones de valoración de la solvencia y las oficinas de crédito. Los prestamistas profesionales estarían excesivamente protegidos, sobre todo en un medio muy informatizado, en el cual podría accederse a una información referente a miles de personas valiéndose de un terminal en el cual grabara el consultante la clave correspondiente.

En general, la intimidad o privacidad de una información personal es función del criterio imperante dentro del medio social en cuanto a lo que deba considerarse privado. Dicho de otro modo, la posibilidad de ejercitar la acción de privacidad depende de la capacidad o predisposición de la comunidad para distinguir los hechos que deban ser considerados como del dominio público y los que no lo son. Los criterios que imperan dentro de un medio social son variables e inestables. En el caso de las actitudes sociales para con la religión o la sexualidad se han

producido cambios radicales en menos de una generación. Ya dentro del contexto informático, la creciente informatización de datos personales, unida a la creciente demanda de datos por parte de los dirigentes va estrechando lentamente la sensibilidad social para con lo que es privado. Es parte de un fenómeno más general de erosión de valores, ligado a la evolución tecnológica: los accidentes de carretera cuestan la vida a varios centenares o miles de personas cada año, y la consecuencia de ello es una indiferencia cada vez más acentuada por parte del público. Del mismo modo, la sociedad tiende a perder el sentido de la privacidad de sus datos personales a medida que se van generalizando las tranmisiones de grandes masas de datos personales. Por otra parte, ciertos conjuntos de datos que individualizadamente serían considerados privados podrían perder tal carácter una vez registrados en un archivo informatizado, en unión de datos inequívocamente públicos. El carácter público de datos relativos a seguridad social, por ejemplo, tiende a comunicarse a los datos médicos confidenciales almacenados en memoria juntamente con aquéllos.

El cuarto de los supuestos básicos definidos por PROSSER es el de la conducta que coloca a otra persona bajo una «falsa luz» ante los ojos del público. En el contexto informático este supuesto sería aplicable si la jurisprudencia ampliara su ámbito a los casos en que una persona se considerara ofendida por haberse difundido una información equívoca acerca de la misma o se hubiera usado una información veraz, pero fuera del contexto adecuado, o la información hubiere llegado a ser inexacta a causa de su antigüedad, de haberse añadido a la misma datos no pertinentes, o si se hubieran omitido al difundir la información datos relevantes en razón del contexto.

Las deficiencias sustantivas y procesales de la «acción de privacidad» han movido a la doctrina norteamericana a buscar otras fórmulas, siempre dentro del marco del concepto de la proteción de la intimidad. Una de tales fórmulas consiste en el intento de construir un derecho dominical sobre la información personal. De admitirse tal derecho, el ofendido dispondría de toda la gama de acciones y remedios previstos para la protección de las relaciones jurídicas de propiedad. Esta construcción,

propuesta por Alan WESTIN, tendría la ventaja de matizar con claridad los límites del derecho, por analogía con las limitaciones del dominio. En cambio, implica una distorsión de unos conceptos jurídicos elaborados con una finalidad distinta; lo que se pretende no es definir el título jurídico justificativo de los derechos sobre la información ni tampoco determinar la persona que tiene el poder de ejercer el control de la explotación mercantil de la información como bien patrimonial. Por otra parte, en el caso de las oficinas de crédito, el concepto del derecho dominical sobre la información supondría admitir la titularidad de un derecho sobre una cosa, el registro o archivo relativo a una persona, que ha sido creada por otra persona. Finalmente, si se reconociera el derecho dominical sobre la información, se cargaría todo el peso de la responsabilidad sobre el titular del derecho, cuando, en realidad, es más importante imponer unos deberes específicos o unas limitaciones a las organizaciones que necesitan y usan los datos.

Otro concepto al que se ha acudido para instrumentar la protección de la privacidad de los datos es el de apropiación ilícita *(misappropiation)*. Este concepto se funda en una sentencia que sentó precedente y dio lugar a una construcción teórica. La sentencia *(International News Service c. Associated Press)* fue dictada por un Tribunal en un caso en el que la parte demandada se había adueñado de noticias de prensa obtenidas por telégrafo y redactadas por la parte actora. Pese a que lo más defendible habría sido fundar el fallo en la competencia desleal, el Tribunal afirmó que la parte actora tenía un derecho «cuasi-dominical» a obtener un justo beneficio del capital y recursos invertidos en su empresa de noticias de prensa. La jurisprudencia posterior amplió el ámbito de esta doctrina a supuestos de «inmoralidad comercial», tales como la imitación de modelos de trajes y la copia de discos de gramófono. Este concepto tiene la ventaja de determinar unos derechos susceptibles de una valoración económica, entre los titulares de la información y los captadores, difundidores y usuarios de ella. A esta ventaja hay que añadir su elasticidad y generalidad. El inconveniente principal que presenta es que tiende a ser utilizado para proteger valores económicos en lugar de valores personales o emocionales. En

todo caso, como el concepto del derecho dominical, implica una distorsión de conceptos jurídicos creados para otros fines.

Finalmente, se ha acudido al concepto de la fiducia o *trust*. Es el criterio seguido expresamente por una organización denominada «United Planning Organization», creada para constituir un banco de datos con información acerca de programas benéficos de instituciones de Wáshington. La UPO obtuvo grandes volúmenes de datos y los colocó en fideicomiso, bajo la dirección de tres fiduciarios. Las condiciones del fideicomiso figuraban en una escritura o instrumento fiduciario en el cual se garantizaba el uso de los datos en la forma convenida y el secreto de los mismos. Esta construcción tropezaría con dificultades derivadas del mismo concepto del *trust*, que, entre otras cosas, exige en lo que se cede en fideicomiso pase a propiedad del fiduciario, lo cual llevaría al mismo resultado de que unos mismos datos podrían pasar a ser de propiedad de distintos fiduciarios, en el caso de que varios bancos de datos optaran por la solución del fideicomiso como garantía de la privacidad de los datos. Lo más grave sería que unos bancos de datos establecieran tal garantía y otros no, con lo que estos últimos podrían abusar impunemente de los datos personales. Por otra parte, el fideicomiso lo crea unilateralmente el banco de datos que almacene los datos personales, sin que los entes intermedios garanticen, a su vez, el secreto a los interesados (al menos, así fue en el caso del UPO).

El concepto de la acción de privacidad, o de *right of privacy*, no es, pues, viable y ello por razones diversas, unas de ellas debidas a peculiaridades del propio sistema norteamericano de elaboración jurisprudencial del Derecho (problemas de carga de la prueba, rigor de los precedentes, lenta decantación de la doctrina jurisprudencial), y otras resultado de la relatividad del concepto mismo de intimidad o información «privada», sin olvidar que la transposición del concepto del derecho de privacidad al contexto informático desnaturaliza en parte los supuestos de hecho definidos por la jurisprudencia al tener que recurrir a otros factores como la infracción de una relación de confianza, etc.

A estos factores hay que añadir que la ausencia de una legislación federal sobre el problema creaba el peligro de que, al quedar a merced de las legislaciones de los Estados, no existiera una unidad en los principios aplicables y la protección de los datos variara en intensidad y eficacia de un Estado a otro. En este ámbito, la homogeneidad y certeza del Derecho ofrecen una importancia especial, debido a la posibilidad de una generalización de las transmisiones masivas a través de líneas y redes multiestatales. Por otra parte, de no existir una legislación federal, los grandes bancos de datos y centros de proceso de datos federales no estarían sujetos a la jurisdicción de los Tribunales estatales.

Las dificultades que en el orden conceptual y jurisprudencial ofrecía la inserción del concepto de la privacidad en el ordenamiento jurídico norteamericano dieron lugar a la promulgación de una Ley especial en 1974. Mediante dicha Ley se modificó el título 5 del código de los Estados Unidos, añadiéndose al artículo o sección 552 un artículo o sección 552 *a*, constituido por nueve subdivisiones o secciones.

Partiendo del axioma de que la privacidad del individuo está afectada directamente por la captación, conservación, uso y difusión de información personal por entes y órganos federales la sección 2 de dicho artículo 552 *a* (a modo de preámbulo de la parte estrictamente normativa) matiza los riesgos que para el individuo representa el uso generalizado de los sistemas de información. Tales riesgos no se limitan a la invasión de la intimidad, sino que comprenden una puesta en peligro de las posibilidades del individuo en cuanto a seguridad en el empleo, beneficios de los seguros y del crédito, así como en cuanto a la efectividad de las garantías jurisdiccionales *(due process of law)*. Asimismo, se afirma en dicha sección 2 el carácter de derecho fundamental del derecho de privacidad.

En esta sección 2, en el apartado *(b)*, se define el ámbito del derecho de privacidad, que debe entenderse en un sentido amplio, por cuanto que comprende otros conceptos, tales como el derecho de acceso, el derecho a exigir que los datos sean utilizados sólo para el fin para el cual fueron obtenidos y el derecho a que la difusión de información personal se limite a los

casos en que tal difusión la exija una finalidad necesaria y legítima. Se incluye asimismo el concepto de derecho de privacidad como derecho del individuo a decidir qué datos pertenecientes al mismo deben ser obtenidos, utilizados o difundidos por los entes y órganos federales (23).

La Ley establece para defender la privacidad (entendida en un sentido amplio) un sistema de control de la difusión y comunicación de los datos personales registrados en ficheros automatizados llevados por entes y órganos de la Administración federal.

3.2.1.2 La noción de la privacidad o intimidad ha sido asimismo recogida, con algunas variantes, en la Ley sueca de protección de datos de 1973.

Dos son los conceptos que se observan en dicho texto. Por una parte, el que se define con la expresión «intrusión en la integridad personal», que podría equipararse al concepto de intrusión en la privacidad definido como uno de los cuatro grandes aspectos del concepto norteamericano de *right of privacy*. Este concepto de intrusión en la integridad personal no se define en la ley sueca. Sin embargo, el artículo 3 condiciona la autorización para crear o explotar un banco de datos personales a la no existencia de motivos fundados para creer que la explotación del banco de datos pudiera dar lugar a tal intrusión. El mismo criterio se recoge en el artículo 11 como condición para autorizar la salida de información del país para su tratamiento en el extranjero. El mismo concepto reaparece en otros preceptos como el artículo 15 y el 19.

Otro concepto de privacidad se recoge en el artículo 4. En este caso no se alude genéricamente a la integridad personal, sino que se enumeran varios supuestos de información personal cuya inclusión en un banco de datos personales da lugar a que sólo excepcionalmente se conceda a particulares autorización para crear o explotar tales bancos de datos. Dichos supuestos tienen en común la presunción de que el afectado no es previsible que consienta su difusión a terceros. Es el caso de que una persona haya sido objeto de tratamiento en instituciones de

(23) Cfr. supra nota 20. Véase el texto completo de la ley en el apéndice documental de este trabajo.

protección de menores, o en instituciones de cura del alcoholismo, de tratamiento psiquiátrico, de tratamiento de ciertas perturbaciones psíquicas, o bien que haya sido objeto de medidas de represión de la asocialidad o peligrosidad social, o de medidas previstas en la legislación de extranjería. También los datos referentes a la confesión religiosa o ideas políticas quedan comprendidos en esta noción de intimidad o privacidad. En todos estos supuestos es preciso probar que existe un motivo especial para crear o explotar el banco de datos personal, para poder obtener la autorización. Esta exigencia sólo afecta, como queda dicho, a los bancos de datos privados. Por consiguiente, habrá que entender que si se trata de un banco de datos público creado y explotado por un órgano estatal dentro del ámbito de su respectiva competencia no será de aplicación este condicionamiento.

En cualquier caso, la ley sueca no aporta nada en el orden conceptual. Pues, por lo que respecta al primero de los conceptos aludidos, deja a la discreción de la Administración (concretamente, la Inspección de Datos) la decisión de determinar cuándo existe el riesgo de una intrusión indebida en la integridad personal, lo cual implica que, hasta tanto se disponga de una jurisprudencia o de una casuística suficientemente abundantes no será posible elaborar este concepto, por vía de inducción o a partir de formulaciones específicas. En cuanto al segundo de los conceptos que parecen estar presentes en la mente del legislador sueco, los distintos supuestos en que se refleja son considerados aisladamente y en ningún momento se les hace derivar de ninguna otra noción genérica de la que pudieran ser corolarios. La ley hace remisión en cada caso a la respectiva definición legal de cada supuesto.

3.2.1.3 *Limitaciones del derecho de privacidad.*—El concepto de intimidad o privacidad ha sido el más comúnmente aceptado, al menos en un primer momento de máxima inquietud. Así sucedió en los Estados Unidos en 1967, en que se proyectó la creación de un National Data Center.

Sin embargo, dejando aparte las dificultades que la modulación del concepto de «derecho de privacidad» encuentra en el

Derecho norteamericano, este concepto no es válido como medio de obtener reglas jurídicas que permitan proteger la información. A ello hay que añadir la desmesurada extensión que confieren al concepto algunos juristas. Así, Colin TAPPER (24) considera que constituye invasión de la intimidad el uso de los datos personales para una finalidad distinta de aquélla para la cual fueron obtenidos.

El solo análisis de este concepto ha conducido a la conclusión de su escasa viabilidad normativa, sobre todo por su fácil conflictividad con el interés público. El supuesto más expresivo al respecto lo constituyen los datos referentes al historial médico de una persona: si, en aras de la protección de la intimidad, se limita o prohíbe el conocimiento de tales datos por las autoridades sanitarias, será imposible o difícil emprender campañas de prevención médica que beneficien a amplios sectores de la población. El ulterior análisis de las diversas cuestiones implicadas ha conducido, de una parte, a formular otros principios más viables (derecho de acceso, regla de la racionalidad del uso de los datos, etc.), y, por otra, a cargar el acento, no tanto en la defensa de la intimidad, como en la necesidad de un control de la información registrada, tendiendo así a instrumentar, mediante las formas clásicas de intervención administrativa, una protección indirecta de los diversos bienes jurídicos implicados.

En términos parecidos se pronuncia el informe francés «Informática y Libertades» (25), redactado por una comisión de igual nombre como resultado de una campaña de prensa motivada por el proyecto S. A. F. A. R. I. Se trataba de un proyecto informático consistente en el establecimiento de una clave de identificación para todos los franceses. Tales claves, o identificadores universales, tienen por función servir de charnela entre los diversos ficheros, haciendo posible su interconexión y el acceso casi instantáneo a todos ellos. Si bien sólo se trataba de una posibilidad técnica, ya que dicho acceso (casi) instantáneo requería una situación de plena informatización de los ficheros

(24) TAPPER, C.: *Computers and the Law*, Londres, Weidenfeld & Nicolson, 1973, página 37.

(25) París, *La Documentation Française*, septiembre 1975.

personales, se produjo una gran inquietud en Francia, alentada en parte por la poco afortunada designación del proyecto (26).

Esta inquietud tenía su base en el riesgo de invasión de la intimidad que el acceso a los ficheros de datos personales podía llevar consigo. La Comisión aludida fue designada para dictaminar sobre los peligros que para la vida privada representaba la posible interconexión de ficheros. A tal efecto fueron suspendidas las conexiones de los ficheros públicos, hasta tanto la Comisión emitiera su informe. Este, sin embargo, derivó hacia una problemática totalmente distinta.

El informe dice textualmente: «La protección de la vida privada frente a la colecta, el tratamiento y la circulación abusivos de ciertas informaciones ha sido una de nuestras preocupaciones dominantes. Pero no hemos tenido que intentar definir lo que es la vida privada, porque nuestra misión no se detenía en modo alguno antes tales fronteras.» «De no haber sido así, el legislador sentiría la sensación de haber hecho una labor liberal, por cuanto que los secretos y la tranquilidad del individuo y quizá también los de la unidad familiar estarían protegidos, en tanto que los derechos y libertades del ciudadano que participa en la vida pública, del trabajador que desempeña su puesto o depende del mercado de trabajo, del dirigente de empresa, de las asociaciones, sindicatos y partidos políticos podrían verse comprometidos.»

Tampoco creyó deber limitarse al estudio de los problemas del tratamiento de la información «nominativa», noción más amplia que la de la vida privada, pese a que tal tipo de información es especialmente vulnerable si se la contempla dentro de la óptica de las libertades. Pero es que, si bien los archivos nominativos pueden aprehender al individuo en la totalidad de sus actividades políticas, sindicales, profesionales, y asimismo registrar todo lo referente a las empresas y grupos, los ficheros o archivos no nominativos pueden pesar, aunque indirectamente, sobre la suerte de los individuos y grupos y reducir de hecho sus libertades.

No obstante lo antedicho, el proyecto francés en que han cristalizado las conclusiones del informe de la comisión no ha

(26) La sigla SAFARI (Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus) dio lugar a artículos de prensa como el aparecido en *Le Monde:* «SAFARI. La chasse aux français» (ed. de 21 de marzo de 1974).

renunciado al concepto de la intimidad, si bien confiriéndole una fisonomía distinta. Su artículo primero sienta el principio general de que «la informática debe desenvolverse respetando la vida privada y las libertades públicas e individuales».

3.2.2 *El derecho de acceso a los datos.*—Un planteamiento distinto del problema ha conducido a la formulación de otro concepto: el derecho de acceso. Según observa BRAIBANT (27), el desarrollo de la informática debe ir acompañado de una ampliación del derecho a la información. Es decir, si el desarrollo del tratamiento automático de datos puede dar lugar a un aumento del poder sobre el individuo, hay que compensar este aumento de poder mediante una intensificación del derecho a la información.

Pero este derecho a la información debe ser acotado debidamente. La necesidad de su ampliación surge de la proliferación de los archivos informatizados de carácter nominativo. Es preciso que el interesado conozca los datos que hay registrados acerca de él y en los cuales hayan de fundarse decisiones que le afecten. Pero ello debe ir unido al secreto de los datos que afecten a los demás. En rigor, no es algo enteramente nuevo. Nuestra ley de procedimiento administrativo de 1958 ya estableció el derecho de los interesados en un procedimiento administrativo a conocer el expediente, pero tal derecho está concebido en términos restrictivos, por cuanto que se constriñe a la existencia de un expediente en tramitación. Los artículos 62 y 63 no serían de aplicación al supuesto de una mera petición de información acerca de los datos incluidos en un fichero o archivo con relación a una persona dada. En Francia, una ley

(27) BRAIBANT, G.: «Le droit d'accès des citoyens à leurs dossiers personnels», en *Questions d'ordre politique soulevées par la protection des données*, OCDE, Etudes d'Informatique, vol. 10, 1976. La preocupación por la defensa de la intimidad lleva a algún jurista a incluir en el concepto de privacidad el llamado *habeas data*. Así, MILLER, que sostiene que la creación en el Derecho norteamericano de una acción o breve de *habeas data*, a modo de sucedáneo del *habeas corpus* implica una distorsión de un remedio jurídico concebido para una situación muy distinta. «Un remedio judicial creado hace más de ochocientos años para proteger a un individuo que ha sido encarcelado, ordenando que sea llevado ante un tribunal, si bien presenta una interesante analogía, ofrece poco que sea relevante en la búsqueda de una estructura jurídica para proteger la información personal registrada en ordenador. Llenar nuevos odres con viejos vinos raras veces da un producto gustoso.» (MILLER, A. R.: *The assault on privacy*, Signet Books, 1972, p. 231.)

de 22 de abril de 1905 (28) estableció la obligación por parte de la Administración, de poner de manifiesto el expediente en caso de procedimiento disciplinario incoado contra un funcionario. También en este caso, el derecho de acceso está limitado al caso del expediente sancionador. Es necesaria, por tanto, una formulación genérica, independiente de cualesquiera condicionamientos específicos.

La doctrina ha definido el contenido de este derecho de acceso en términos generales, y, para evitar equívocos, lo ha bautizado con el nombre de *habeas data* o *habeas scriptum*, recordando la denominación del viejo breve de *habeas corpus*. Si el fin de éste es forzar a una persona que ilegalmente detiene a otra, a que «entregue el cuerpo», el *habeas data* aspira a obligar a una persona o entidad que tiene registrados datos de otra persona, a que exhiba o ponga de manifiesto a ésta los soportes informatizados en que se contengan tales datos (29).

El derecho de acceso ha sido ya objeto de una elaboración conceptual suficientemente perfilada. La doctrina distingue dos órdenes de cuestiones: el *sujeto* del derecho y el *objeto* del derecho. Por lo que respecta al sujeto, es evidente que se trata de un derecho personalísimo, lo cual da lugar a un problema técnico, de identificación, en los supuestos en que el archivo consultado se halle a gran distancia y sea preciso consultarlo por correo o por teleproceso. También puede originar un problema de índole más estrictamente jurídica, cuando el interesado trate de consultar el archivo por medio de un mandatario; en este caso habrá que adoptar medidas para evitar que el mandatario, a su vez, cree unos archivos con los datos de sus clientes.

El objeto del derecho de acceso, la doctrina propugna que comprenda no sólo los datos en sí mismos, sino además las *fuentes* de los mismos y los *usos* que de ellos se hagan. Los textos legislativos existentes sólo precisan la obligación de informar de las fuentes en los casos de empresas dedicadas a emitir informes valorativos sobre la solvencia.

(28) Citada en BRAIBANT, G.: *Loc. cit.*

(29) La fórmula o principio *habeas scriptum* se debe a G. B. F. NIBLETT: *L'information numérique et la protection des libertés individuelles*, Etudes d'Informatique, vol. 2, París, OCDE, 1971.

Entendido así el derecho de acceso, se desprenden de él dos corolarios. En primer lugar, la necesidad de que el interesado conozca la existencia del archivo o fichero y de los datos. Esto implica, a su vez un acto específico de notificación al interesado, o bien la publicación de la creación del archivo, mediante anuncio en el diario oficial o en periódicos de mayor tirada de la localidad respectiva.

El otro corolario lo constituye el derecho a impugnar los datos incompletos, inexactos, obsoletos o ilícitos, y la correlativa obligación del titular del archivo, de rectificar tales datos. Este derecho tiene en la práctica formas diversas de aplicación, según que los datos consistan en hechos no susceptibles de interpretación, o en juicios valorativos. En el primer supuesto cabe la fórmula adoptada por Francia en una ley de 1970, reguladora de los ficheros de conductores: trasladar la carga de la prueba al responsable del fichero en casos de impugnación de la veracidad de los datos; en algunos supuestos no es posible tal prueba, cuando la misma hace referencia a hechos tales como el haber estado en un lugar determinado el día X. En el caso de que los datos consistan en juicios de valor, cabe que el interesado aporte una declaración, que sea luego unida a su expediente y comunicada a terceros. Algunos de los textos existentes, completan este cuadro de garantías, con la regla de que las rectificaciones, adiciones o supresiones de datos, resultado de la impugnación, sean comunicadas a las personas que habían tenido conocimiento de los datos inexactos, incompletos o falsos, con objeto de que tales personas puedan, a su vez, modificar sus decisiones o su actitud para con el interesado. Esta obligación se suele limitar a un determinado período de tiempo anterior: es decir, si los datos inexactos o incompletos habían sido comunicados a terceros con una anterioridad superior a un plazo dado (contado en sentido retroactivo a partir de la resolución de la impugnación), no es preciso comunicar la rectificación (30).

La regulación más precisa es la que se contiene en la proposición de ley de la Cámara de Representantes norteamericana (H. R. 2998) por la que se modificaba el Código de los Estados

(30) Ver un estudio general del derecho de acceso en BRAIBANT, G., OCDE, *Questions...*, 1976.

Unidos, título 5, capítulo 5, subcapítulo II, añadiendo a continuación de la sección 552 una nueva sección 552a. Objeto de la regulación propuesta era precisamente el derecho de acceso. Preveía solamente el supuesto de la puesta de manifiesto, de oficio, de los registros con datos personales.

Los registros habrían de hacer referencia a personas determinadas, bien con ayuda del nombre respectivo, bien por medio de un identificador numérico o simbólico. Asimismo, la información registrada debía proceder de fuente que no fuera la propia persona interesada. Tales registros habrían de ser puestos en conocimiento de los interesados, comunicándoles primero la existencia de los mismos, y permitiéndoles examinarlos, completar información, retirar información errónea. Asimismo, se preveía que el órgano o autoridad llevara un registro de las personas a las cuales se hubiera divulgado información contenida en tales registros, así como los fines de dicha divulgación. Quedaban exceptuados los registros referentes a personas incursas en investigaciones policiales.

Asimismo, el proyecto francés, estructurado en seis capítulos, dedica el capítulo IV al «Ejercicio del derecho de acceso», regulando en el mismo lo referente al sujeto (artículo 27), objeto (ibídem), contenido (obligación de comunicar los datos, art. 28; derecho de rectificación, adición de datos para completar la información, aclaración o cancelación, art. 29), competencia (artículo 30) y modalidad especial en el caso de los datos médicos (comunicación a través de un médico designado al efecto por el interesado, art. 31).

3.2.3 *El uso de los datos según su finalidad.*—Otro principio recogido en la normativa legal ya existente es el de que los datos que han sido obtenidos para un determinado fin no deben ser usados para un fin distinto. Es decir, si un banco de datos contiene datos de carácter médico, que han sido solicitados y registrados con el fin de facilitar la obtención de historiales o antecedentes médicos, o de prevenir determinadas enfermedades, no sería lícito utilizar tales datos para una finalidad que no fuera la prevista. Este principio es realmente importante y

podría considerarse suficiente como medio de proteger los diversos bienes jurídicos puestos en peligro por la informática.

Este principio ha sido recogido expresamente en la *Privacy Act*. La sección 2 (b) de la misma (que contiene la parte equivalente a una exposición de motivos) señala entre los fines de la ley el de establecer unas medidas de protección del individuo contra la invasión de la privacidad, exigiendo a tal efecto a los entes y órganos federales que, salvo disposición legal en contrario,

«... permitan al individuo impedir que los datos referentes al mismo, obtenidos por tales entes y órganos para una finalidad concreta, sean usados o puestos a disposición para otra finalidad sin su consentimiento».

Más radical es el artículo 35 del proyecto francés. En éste se tipifica como delito la conducta de quien, disponiendo de datos personales («nominativos») con ocasión de su registro, clasificación u otra forma de tratamiento de los mismos, «... los hubiere desviado de su finalidad». A este efecto, se considera como finalidad la que figurare como tal en la resolución administrativa aprobatoria del tratamiento o tratamientos interesados.

3.2.4. *La regulación jurídica del proceso de datos.*—En Alemania Federal, el informe del Ministerio federal del Interior sobre protección de datos (31) dice con toda claridad que «el concepto de privacidad o esfera privada no es idóneo para la protección de datos». Considera que el objeto de la protección es sólo la información individualizada, comprendida la relativa a grupos. Sin embargo, sólo el tratamiento de la información da a ésta carácter individual, y es ese tratamiento lo que da origen a unos riesgos específicos. Consecuencia de ello es que la protección de los datos debe ser indirecta, instrumentada a través de una reglamentación del proceso de dicho tratamiento y de sus sucesivas fases, las cuales, a su vez, determinan otros tantos sectores problemáticos o *topoi*. Aparece así una solución más, cuyo obje-

(31) *Grundiragen des Datenschutzes.* Gutachtem im Auftrag des Bundesministeriums des Innern; Deutscher Bundestag, 6. Wahlperiode, Drucksache VI/3826 (septiembre 1972).

to no es la protección de la intimidad, sino la disciplina jurídica del proceso de datos. Esta solución es la que inspira el proyecto alemán federal, los proyectos noruegos y el proyecto francés.

El proyecto francés se funda en consideraciones análogas. Si los trabajos preparatorios estuvieron centrados, al parecer, en los archivos informatizados, el texto definitivo ha prescindido de ellos, estimando que sólo el tratamiento de la información contenida en los archivos da lugar a problemas. Por el contrario, la información que no es objeto de tratamiento no suscita problema alguno. De ahí que el proyecto francés sea un proyecto de ley reguladora del proceso de datos o tratamiento de la información, girando todo su aparato normativo en torno a este criterio.

Dentro de este marco, la normativa del proyecto alemán federal y la del proyecto francés establecen algunas matizaciones en relación con el objeto del tratamiento: archivos públicos, privados, del Estado o entes locales, etc.

La regulación del tratamiento de la información como tal lleva aparejado en el proyecto francés un interesante principio, que hace referencia al valor del resultado de un tratamiento de datos como fundamento de una decisón jurisdiccional o administrativa. El artículo 2 dice:

> «Ninguna decisión jurisdiccional o administrativa que implicare la apreciación de un comportamiento humano podrá tener como único fundamento un tratamiento automático de informaciones.»

Con este interesante precepto se sale al paso de elucubraciones teóricas acerca de la posible automatización de la función jurisdicente. El tratamiento automático de la información permite elaborar datos de hecho, transformándoles en otros datos de hecho. Sin duda existen sentencias judiciales o resoluciones administrativas que pueden fundarse en meros datos de hecho, tales como operaciones aritméticas; es el caso de muchas de las resoluciones de la Administración fiscal. Pero lo normal es que toda decisión, tanto administrativa, como judicial, se funde asimismo en juicios de valor referidos a una conducta humana.

3.2.5 *El derecho al olvido.*—Ya aludimos al principio al problema de las «cárceles informáticas». El registro de determinados datos referentes a una persona puede ser pertinente en un momento dado, pero perder progresivamente actualidad y relevancia, por razones derivadas de la conducta de dicha persona o por factores ajenos. Así, si en un registro policial figura la embriaguez habitual como circunstancia específica de una persona, si el interesado deja de ser borracho habitual es preciso cancelar tal dato, pues ello podría seguir obrando en contra del interesado. Lo mismo sucedería con datos referentes a la experiencia profesional, etc.

Ninguno de los textos prevé este problema expresamente, si bien la propia mecánica del derecho de acceso en su vertiente de derecho de rectificación permite llegar a una solución que evite estas cárceles o cementerios de datos. Ya algunos ficheros manuales, tales como los registros de condenas criminales prevén la cancelación de la inscripción cuando ésta ha llegado a ser irrelevante. Dentro de una óptica *de lege ferenda* convendría tener en cuenta este problema y generalizar esa solución del registro de condenas criminales.

3.2.6 *Aspectos constitucionales.*—Otro posible conflicto de intereses que parece perfilarse es el que resulta de la necesidad de la protección de los datos y la de conservar los principios constitucionales.

Esta cuestión fue objeto de un precepto en la Ley de Protección de Datos del Estado de Hesse, de 7 de octubre de 1970. El artículo 10, apartado 2, encomienda al Interventor de Datos la función de observar las repercusiones que el tratamiento de la información pudiere tener sobre las competencias decisoras de las autoridades administrativas, «determinando si tales repercusiones conducen a un desajuste en la división de los poderes entre los órganos constitucionales del Estado» y entre los órganos de la Administración.

El problema ha reaparecido en el informe Tricot, de la Comisión «Informática y Libertades», base, en lo esencial, del proyecto francés. La cuestión se centra en la posibilidad de que el Ejecutivo, con sus grandes ficheros o bancos de datos, llega

a gozar de un verdadero monopolio de la información en determinados ámbitos de la actividad política, económica o social. Dentro del marco de un régimen parlamentario, este monopolio puede dificultar, si no impedir, el control del Ejcutivo por el Parlamento.

Para salir al paso de este problema, la versión inicial del proyecto francés contenía un artículo que no figura en la versión actual, en el cual se ampliaba a los órganos constitucionales el derecho de acceso. El precepto decía así:

> «La igualdad de acceso de los Poderes públicos a las informaciones automatizadas de interés general, de orden estadístico o documental, deberá ser respetada, a fin de no atentar al equilibrio democrático previsto por la constitución entre las instituciones de la nación.»

zón de que este artículo haya sido suprimido estriba en que, a juicio de los redactores del proyecto, la cuestión a que hace referencia debía ser objeto de un proyecto especial, habiéndose creado a tal efecto una comisión de estudio presidida por LUCIEN MEHL (32).

El expresado artículo establecía un nuevo principio, el de *igualdad* (33). Su instrumentación puede llevarse a cabo acudiendo a un concepto recogido en el Derecho del procedimiento administrativo y que se conoce con el nombre de «auxilio administrativo», constituyendo una transposición al procedimiento administrativo de la institución procesal del auxilio judicial. La Ley Fundamental de Bonn contiene en su artículo 44, apartado 3, la regla de que los órganos judiciales y administrativos deben prestarse entre sí auxilio judicial y administrativo *(Rechtshilfe, Amtshilfe)*. Quizás no sea del todo necesario regular esta cuestión a nivel constitucional, pero en cualquier caso debería prestársele la debida atención, ya que la informatización de los ficheros de los órganos de la Administración ha hecho viable la interconexión de dichos ficheros. Asimismo, el concepto de auxilio entre órganos, limitado hasta ahora en la doctrina a los órganos administrativos y judiciales, debe hacerse extensivo a los

(32) JOINET, L.: *Le projet de loi français rélatif à l'informatique et aux libertés*, en la documentación de las V Jornadas Hispano-Francesas de Informática (Madrid, 1976, ed. multicopiada).

(33) Cfr. BRAIBANT, G.: *Informatique et libertés publiques*, ibídem.

órganos legislativos, tales como las comisiones o comités o a las Cámaras. Es el criterio que sigue el artículo 6 de la ley de Hesse.

Otro principio que ha sido formulado en relación con la problemática constitucional es el de la *transparencia* (34). Este principio hace referencia, en realidad, a las garantías de las libertades públicas. Las libertades y los derechos públicos subjetivos requieren, para poder ser ejercidos, la existencia de unos registros o ficheros debidamente accesibles y conocidos por los interesados. Para lograr esto podría instituirse la obligatoriedad de unos trámites de información pública en todo supuesto de creación de un fichero público que incidiera en el ejercicio de las libertades individuales y públicas.

3.2.7 *Los problemas de la circulación transnacional de la información.*—Otro ámbito sobre el cual incide la problemática de la protección de datos es la circulación transnacional de éstos, tema objeto de múltiples estudios por parte de organizaciones internacionales (OCDE, Consejo de Europa, etc.).

En rigor, esta circulación transnacional de datos no es una novedad. En la época preinformática ya se transmitían datos de un país a otro en formas diversas, sobre todo si consideramos como tales transmisiones la radiodifusión o la televisión. La informatización de los archivos ha tenido como consecuencia un más fácil acceso, un contenido más rico y la posibilidad de usos múltiples, simultáneos o no, de los datos registrados. El progresivo uso de las telecomunicaciones ha tenido también su impronta en la transmisión transnacional de datos. El caso mas conocido de tal transmisión lo constituye la difusión de la información meteorológica, con miras a facilitar la previsión de la evolución de los movimientos atmosféricos. Hoy día, la información meteorológica se transmite instantáneamente, pudiendo conocerse con una fidelidad casi absoluta en cualquier momento el mapa del tiempo de una región dada; esta transmisin se realiza en forma digital, por medios ordinarios o vía satélite. Otro supuesto, que tampoco es nuevo, es el de las consultas a los archivos de la Interpol o las peticiones de búsque-

(34) Cfr. BRAIBANT, G.: *Loc. cit.*

da de delincuentes hechas por conducto de esta organización. Sin embargo, hoy, con la informática, ha sido posible crear grandes bancos de datos policiales internacionales por parte de la Interpol, así como el acceso por la misma a los archivos policiales nacionales. La utilización generalizada de la informática hará posible la creación de un sistema internacional de control de pasaportes. Asimismo, dentro de ámbitos regionales específicos, como los países escandinavos, por ejemplo, se tiende a crear unos bancos de datos que apoyen el sistema de mercado de trabajo y de seguridad social común que de hecho existe entre tales países. También es posible en épocas de elecciones que los residentes en otros países emitan su voto utilizando los medios de transmisión, con la ayuda de los archivos de población informatizados.

Todos estos supuestos se encuadran fácilmente en el concepto de auxilio administrativo internacional. El auxilio judicial internacional (exhortos, comisiones rogatorias, peticiones de extradición, etc.) no ha sido hasta ahora objeto de una informatización, pero ésta puede producirse en un futuro más o menos próximo. A este respecto, existe ya una infraestructura de información en los archivos de la Interpol, que podría ser adaptada sin dificultad a las necesidades de los procedimientos informatizados. Ni el auxilio administrativo ni el judicial suscitarían problema especial alguno por el solo hecho de su informatización.

El problema surge en otro plano. La interdependencia existente entre las economías de algunos países geográficamente próximos da lugar a que el país mejor dotado de equipos informáticos almacene datos sobre los recursos industriales, agrícolas, geológicos, etc., de los países vecinos. Es el caso de los Estados Unidos con respecto al Canadá. En los últimos años ha surgido en el Canadá un creciente temor ante la existencia de bancos de datos canadienses en los Estados Unidos. La prensa canadiense ha llegado a hablar de «invasión del Canadá por los Estados Unidos mediante los bancos de datos» (35). El proceso

(35) Gotlieb, A.; Dalfen, Ch.; Katz, K.: «The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approaches to Guiding Principles», *The American Journal of International Law*, vol. 62, núm. 2, abril 1974, página 245, notas.

viene a ser el tradicional de exportar materia prima (datos industriales, geográficos, etc.) e importar un producto acabado (informes estadísticos, prospecciones de mercado, etc.). Los datos ya elaborados pueden ser registrados en bancos de datos, cuya información se consulta mediante un régimen de suscripción o análogo. De estos hechos resulta la problemática específica de la difusión transnacional de datos. Sin perjuicio de una regulación convencional, o como correctivo de la misma, se han formulado respuestas diversas.

Una primera respuesta a estos problemas ha sido la de transponer a la esfera internacional el problema de la intimidad. Paralelamente a la intimidad de las personas existiría una intimidad nacional (36). Esta tesis no ha tenido gran aceptación. Podría inspirar normas de carácter penal, tipificadoras de delitos informáticos específicos, pero en tales casos surgiría el problema de su persecución, ya que sería difícil determinar si tales delitos habían sido cometidos en territorio nacional o en territorio extranjero. Fallaría así el principio de la *lex fori delicti commissi*.

Mayor interés ofrecen otras teorías formuladas al respecto, también como correctivos de cualquier posible regulación convencional. Dichas teorías toman como base las nociones de la *soberanía* y de la *identidad* cultural nacional. La idea de la soberanía figura ya como excepción a la aplicación de la actual Convención Internacional de Telecomunicación (37). En el caso de la informática, la doctrina internacionalista considera que la información es también objeto de la soberanía de los Estados, en tanto en cuanto que un Estado como organización precisa de una determinada información para poder adoptar sus decisiones. De ahí resulta el derecho del Estado a limitar o vigilar la salida de ciertas informaciones, en especial cuando las mismas hagan relación al interés público, a la seguridad, etc.

La pérdida de la identidad cultural es una de las posibles consecuencias de la traslación del poder decisorio a un ámbito territorial ajeno. El ejercicio extranacional de dicho poder de-

(36) *Loc. cit.*, pp. 233 y 234.
(37) *Loc. cit.*, pp. 228.

cisorio implica la aceptación forzosa de las normas culturales que el uso de tal poder refleja (38). Se produce un fenómeno de homogeneización cultural análogo al que crean la televisión y la radiodifusión.

Por lo que respecta a la regulación internacional, bilateral o multilateral, existen ya algunos textos, tales como recomendaciones del Consejo de Europa [Resolución (73)22], y un borrador, elaborado en una reunión celebrada en Oslo, de Convenio Nórdico de Difusión Transnacional de Datos. Asimismo hay que mencionar la intensa actividad desplegada a este respecto por la OCDE (39). Esta regulación convencional no es, sin embargo, obstáculo a que las legislaciones nacionales adopten un mínimo de medidas legislativas en el sentido antes expuesto, de correctivos de un libre flujo transnacional de los datos. Estas medidas podían estar constituidas por unas autorizaciones administrativas previas que habría que exigir, bien para «exportar» datos, bien para recibir determinadas «importaciones». De los textos existentes, sólo la ley sueca y el proyecto austríaco se hacen cargo de este problema de la necesidad de normas de derecho interno para controlar la salida de datos a territorio extranacional. El artículo 11, primer párrafo, proposición segunda, dispone que cuando existe motivo fundado para estimar que la información personal contenida en un fichero o archivo va a ser empleada en un tratamiento de datos que tenga lugar en el extranjero, será precisa la conformidad de la inspección de datos para que pueda facilitarse tal información. A su vez, la inspección de datos sólo puede dar su conformidad a esta comunicación de información si ello no implica invasión de la intimidad («intrusión indebida en la integridad personal»).

El artículo 25 del proyecto austríaco prevé un supuesto más específico. Se trata de la posibilidad de que un ente de Derecho público no sujeto al Derecho austríaco y radicado en Austria (o sea, al parecer, la Organización Internacional de Energía Atómica, con sede en Viena) utilice centros de proceso de datos situados fuera del territorio austríaco, con el fin de elaborar

(38) *Loc. cit.*, pp. 246-248.

(39) OCDE, *Transborder data flows: issues and implications* (DSTI/CUG/76.9). También VILLANUEVA, R., y GARZÓN, G.: *Difusión transnacional de datos*, ponencia de las V Jornadas Hispano-Francesas de Informática (v. nota 32).

datos personales. En tal supuesto, el ente interesado deberá acomodar tal elaboración a sus fines institucionales, no pudiendo, por tanto, elaborar tales datos personales para fines distintos. Asimismo, la elaboración de los datos debe respetar la vida privada y familiar de los interesados.

Un último problema, aunque no menos importante, estriba en el concepto de «transmisión de datos». Sin duda alguna, si se limita tal concepto al transporte de datos por redes de cables, o por líneas específicas, quedarían burladas las precauciones que los acuerdos internacionales proyectados, o los textos internos establecen. De ahí la conveniencia de hacer extensivo el concepto a cualquier forma de envío de datos registrados en cualquier soporte. Así, por ejemplo, el envío por correo de una cinta magnética grabada con un banco de datos entero quedaría comprendido en el concepto de transmisión de datos.

3.2.8 *La intervención administrativa.*—El primitivo propósito de defender la intimidad de las personas resultó ser inviable, del mismo modo que cualquier otro criterio de protección de uno o varios bienes jurídicos en concreto. El análisis atento del tema condujo a configurar tal protección como un control del uso de la información. Con el control de dicho uso se estimó que se protegerían indirectamente los diversos bienes jurídicos implicados: la vida privada, el interés público, las libertades individuales y públicas, la seguridad nacional, etc. Por ello, los distintos textos legales referentes a esta materia, en vigor o en proyecto, establecen un régimen de intervención administrativa. Este régimen reviste formas diversas, susceptibles de una clasificación, al menos a efectos expositivos (40).

Un primer grupo de textos y proyectos es el que prescribe una previa autorización administrativa o licencia para aquellos casos en que se aspira a crear o explotar ficheros o archivos con información acerca de personas. Es la solución de la ley de datos sueca (arts. 2 a 7), de los proyectos noruegos, de la nonnata *Personal Information Act* británica y del proyecto fran-

(40) Cfr. TRUYOL, A., y VILLANUEVA, R.: «Derecho a la intimidad e informática». *Información Jurídica* núm. 318, pp. 113 y ss. Asimismo, LÓPEZ-MUÑIZ, M.: *La intervención administrativa en los bancos de datos*, ponencia de las V Jornadas Hispano-Francesas de Informática (v. nota 32).

cés (art. 12). En estos textos la intervención se encomienda a un ente administrativo colegiado. La autorización se concede siempre que no existan motivos fundados para estimar la existencia de un riesgo de invasión de la intimidad. Sólo la *Personal Information Act* atribuía al órgano interventor una plena discrecionalidad al respecto.

La intervención administrativa no se limita en estos textos a una mera resolución de concesión o denegación de la autorización, sino que dicha resolución contiene además unas instrucciones drigidas al titular del fichero o archivo de datos personales, en las que se regulan los distintos aspectos del tratamiento de los datos, medidas de seguridad, formas de acceso, etc. El sistema más perfilado a este respecto es el de la ley sueca (artículos 6 y 7). También el proyecto francés prevé la posibilidad de unas normas reglamentarias como parte de la resolución autorizante (art. 18).

Un segundo grupo comprende los textos que no exigen la previa autorización, pero prescriben la obligación de declarar a la Administración la existencia de los ficheros o archivos. Es el caso de la *Data Surveillance Bill* británica, el proyecto francés en lo que respecta a los tratamientos de datos llevados a cabo por particulares o entidades privadas y el proyecto danés en relación con los registros de personas llevados por entidades de información crediticia. Un sistema que combina la declaración o denuncia con las normas reglamentarias es el de la *Privacy Act* norteamericana de 1974. El proyecto alemán federal se alinea dentro de este grupo, en cuanto que exige solamente la denuncia o declaración *ex post*, si bien, al igual que el proyecto austríaco, no crea un órgano fiscalizador específico, sino que atribuye la competencia de control a las autoridades de tutela o fiscalización general de las que, respectivamente, depende el ente interesado.

El proyecto austríaco adopta una fórmula peculiar. Distingue entre datos personales almacenados y los bancos de datos, considerando a éstos como una modalidad de explotación de los datos. No prescribe una autorización previa ni una declaración *ex post*. Solamente fija unos requisitos para que los datos personales almacenados por un ente público puedan ser explotados

como bancos de datos. El control o fiscalización del ente que explota tales datos no se atribuye tampoco a un órgano *ad hoc*, sino al ministro del que depende jerárquicamente el ente. Tal control o fiscalización se concreta en la emisión por el ministro de un «Reglamento del banco de datos», cuyas circunstancias precisa el artículo 9 del proyecto.

Otros textos instituyen un órgano de vigilancia análogo a una especie de *ombudsman* especializado. El caso más perfilado es el de la ley de protección de datos de Hesse (art. 10). El proyecto francés (art. 4) atribuye esta función a la Comisión Informática y Libertades.

3.2.9. *Los delitos informáticos* (41).—Independientemente del establecimiento de unas sanciones administrativas y penales, tendentes a dotar de los necesarios dispositivos coercitivos a las imperativas correspondientes, algunos de los textos, en vigor o en proyecto, tipifican supuestos específicos en infracciones criminales fundados principalmente en la especificidad del medio de comisión, en este caso el uso del ordenador o de la información contenida en los ficheros o archivos. La mayoría de los tipos constituyen variantes de otros ya existentes (apropiación indebida, divulgación de secretos). Como delito específicamente informático cabe citar el tipificado en el artículo 35 del proyecto francés: utilización ilícita de datos personales para una finalidad distinta de aquella para la cual fueron obtenidos *(détournement illicite des informations nominatives)*.

Una peculiaridad a este respecto la constituye la *Privacy Act* norteamericana, que, al lado de unas infracciones criminales específicas, prevé unos remedios en vía civil tendentes a forzar a un órgano administrativo a modificar un registro, en virtud del ejercicio del derecho de acceso. Esta peculiaridad obedece, en realidad, a la inexistencia de un régimen de recursos administrativos análogos al de los países europeos.

3.2.10 *Aspectos orgánicos.*—La diversidad de formas de intervención administrativa que se aprecia en esta visión pano-

(41) Cfr. la ponencia expuesta por Córdoba, D., con el título *La informática y el Derecho penal*, en las V Jornadas Hispano-Francesas de Informática (v. nota 32). Cfr. también Parker, D. B.: *Crime by computer*, Ch. Scribner's Sons, 1976.

rámica impide, sin duda, pretender propugnar una forma óptima de estructura orgánica para el órgano o ente público que deba asumir la titularidad de tal intervención. Nos llevaría muy lejos enjuiciar la adecuación de la forma de organización que cada texto, en vigor o en proyecto, prevé, en relación con la específica configuración que confiere a la función interventora.

En todo caso, parece como más conveniente la solución de no adscribir esta función a un órgano ya existente, sino crear un órgano específico, lo más independiente posible, no subordinado a ningún Departamento en concreto. Se tiende a considerar como especialmente apta la solución sueca, noruega y danesa, de una Junta o Consejo, dotada de un órgano permanente en el que se delega la totalidad de la competencia, sin perjuicio de avocaciones concretas. Es la fórmula que también recoge el proyecto francés.

4. La situación del problema en España

En las páginas que anteceden hemos tratado de ofrecer una visión panorámica del movimiento legislativo y doctrinal que constituye la réplica del jurista al reto de la informática, que, en rigor, sólo es una parte del reto de la tecnología en general. Con esta visión panorámica no hemos pretendido, en modo alguno, agotar los aspectos del tema, sino simplemente contribuir a mentalizar al lector acerca del mismo. La mentalización es necesaria, por cuanto que se trata de un problema cuyo planteamiento exige una reacción del individuo frente a las supuestas bendiciones de la tecnología actual. Sólo una vez que se haya producido una «concienciación» en este sentido, cobrará el problema su exacto perfil. No se trata, pues, de «crear» un problema inexistente, sino de impedir que, por ignorancia de los propios derechos y de las consecuencias de una informatización incontrolada, el individuo carezca de una clara conciencia al respecto.

En nuestro país no existe todavía una conciencia generalizada de este problema. No obstante, es interesante observar que,

con independencia de toda información sobre el mismo, se ha visto la necesidad de unas actuaciones normativas de carácter preventivo para proteger la vida privada. Dejando aparte pliegos de condiciones o contratos privados en los cuales se ha considerado conveniente incluir cláusulas de protección del secreto de los datos, hay que citar por lo menos dos supuestos en los que la Administración se ha visto obligada, con carácter de urgencia, a adoptar unas medidas precautorias por vía reglamentaria.

El primero de estos supuestos lo constituye la Orden de la Presidencia del Gobierno de 24 de abril de 1970 mediante la cual se dispone la realización de un censo de los ordenadores existentes en el país, tanto en el sector público como en el sector privado. Dado que el método de ejecución que se prevé consiste en la obtención de los datos directamente a partir de los usuarios, el artículo 3.º precisaba que la Administración puede solicitar datos relativos a los equipos y sistemas de explotación, pero sin que en ningún caso tales datos pudieran hacer referencia a la información contenida en los archivos o registros y elaborada por los equipos o sistemas.

El segundo de los supuestos mencionados lo constituye la Orden del Ministerio de Comercio de 15 de septiembre de 1973, que prescribe la obligación de los comerciantes mayoristas de facilitar al Ministerio de Comercio ciertos datos relativos al suministro y comercialización de productos alimentarios en los mercados mayoristas y establecimientos de venta al por mayor, con miras al tratamiento de dichos datos en uno de los centros de proceso de datos del Departamento. El artículo 4.º precisaba que los datos obtenidos de los comerciantes mayoristas serían tratados de una manera rigurosamente reservada.

Este es, sin duda, el momento idóneo para estudiar el tema en profundidad, con objeto de evitar que, en su día, haya que acudir a improvisaciones. En este primer momento, la Administración podría ordenar un conjunto de estudios coordinados, enderezados a analizar las distintas facetas del problema. Tales estudios deberían comprender, ante todo, una encuesta sociológica proyectada sobre los distintos centros de proceso de datos.

públicos y privados, con el fin de determinar el grado de «concienciación» existente. Al mismo tiempo sería conveniente analizar los niveles de seguridad física y lógica de los centros. Finalmente, procedería una observación continuada y atenta del movimiento doctrinal y legislativo de los distintos países, tanto en el aspecto del Derecho interno como en el del Derecho internacional (42).

(42) En todo caso, la Administración no se halla al margen de estos problemas. Los servicios competentes de la Presidencia del Gobierno siguen con toda atención el movimiento legislativo y doctrinal, participando activamente en las diversas actuaciones que la OCDE, el Consejo de Europa y otros organismos internacionales, así como diversas Universidades y organizaciones privadas, llevan a cabo actualmente. No se puede tampoco desconocer la labor de la Escuela Nacional de Administración Pública, al patrocinar, conjuntamente con el Servicio Central de Informática, un seminario especializado que ha finalizado recientemente, fruto del cual ha sido un interesante borrador de anteproyecto de ley, todavía en fase de mera especulación oficiosa. También hay que aludir a este respecto a las V Jornadas Hispano-Francesas de Informática, celebradas en la segunda quincena de octubre del año actual, y que fueron consagradas al examen comparado del tema en los dos países.

APENDICE DOCUMENTAL (*)

1. *Ley de Protección de Datos, promulgada el 7 de octubre de 1970 por el Ministro Presidente del Estado de Hesse (Alemania Federal).*

Sección primera

Protección de datos

ARTÍCULO 1

Ambito de la protección de datos

La protección de datos abarca todos aquellos documentos aprontados para los fines del tratamiento mecánico de los datos, así como todos los datos almacenados y los resultados obtenidos con el tratamiento de los mismos, dentro del ámbito propio de las autoridades del Estado y de las Corporaciones, Instituciones y Fundaciones de Derecho público, sujetas a la tutela del Estado.

ARTÍCULO 2

Contenido de la protección de datos

Los documentos, datos y resultados abarcados por la protección de datos deberán ser obtenidos, comunicados y conservados de tal manera que no pudieran ser examinados, alterados, accedidos o destruidos por personas no autorizadas. En garantía de ello se adoptarán las precauciones personales y técnicas idóneas.

ARTÍCULO 3

Secreto de los datos

1. Está prohibido a las personas que tuvieren confiada la captación, el transporte, el almacenamiento o el tratamiento mecánico de los datos, comunicar a otros las noticias que el en curso de tales acti-

(*) La versión de los textos de las tres leyes ha sido hecha a partir de los respectivos originales alemán, sueco e inglés, por M. HEREDERO.

vidades hubieran adquirido acerca de documentos, datos y resultados; permitir a otros adquirir tales noticias, o hacer posible, en el curso de tales actividades, que otros adquieran tales noticias; en tanto en cuanto no existiere una autorización al efecto, resultante bien de normas jurídicas, bien del consentimiento de aquellos que estuvieren facultados para disponer de los documentos, datos y resultados.

2. La prohibición del apartado 1 no se aplicará cuando las actividades indicadas en el mismo fueren necesarias para evacuar aquellos trámites administrativos o realizar aquellas operaciones técnicas que requiriere la realización del tratamiento de los datos.

3. El deber de observancia de secreto subsistirá aun después de finalizadas las actividades aludidas en el apartado 1.

4. Las limitaciones que se establecen por razón de la protección de datos se entenderán sin perjuicio de las obligaciones de facilitación de información establecidas, en su caso, por las Leyes.

Artículo 4

Derecho a exigir la protección de datos

1. Si los datos almacenados fueren inexactos, el interesado podrá exigir su rectificación.

2. El que por efecto de un examen, modificación o destrucción contrarios a Derecho, o de un acceso contrario a Derecho, sufriere menoscabo en sus derechos, podrá exigir la reposición a la situación anterior, y en caso de existir peligro de ulteriores menoscabos, podrá exigir la cesación de las actuaciones correspondientes.

3. La presente Ley no afecta al derecho de toda persona natural o jurídica a obtener información de conformidad con las leyes vigentes.

Artículo 5

Bancos de datos y sistemas de información

1. Podrán ser facilitados documentos, datos y resultados, con miras a la creación de bancos de datos y de sistemas de información, así como para fines estadísticos, a las autoridades y entidades mencionadas en el artículo 1.

2. En relación con los bancos de datos y sistemas de información, se garantizará que ningún servicio examinará u obtendrá aquellos documentos, datos y resultados, para cuyo examen u obtención no estuviere facultado en virtud de sus competencias.

3. Los datos y registros que no contuvieren indicaciones concretas sobre personas físicas o jurídicas y no admitieren el acceso a tales indicaciones concretas, podrán ser facilitados y publicados si a ello no se opusiere una prohibición legal o el interés público. Como norma general se entenderá que no se opone el interés público al derecho de información que compete a la Dieta Territorial (art. 6, apartado 1).

ARTÍCULO 6

Derecho de información de la Dieta Territorial y de los órganos de representación municipal

1. La Central de Tratamiento de Datos de Hesse, los centros municipales de cálculo y las autoridades territoriales que explotaren sistemas para el tratamiento de la información deberán facilitar a la Dieta Territorial, al Presidente de la Dieta Territorial y a los grupos parlamentarios de la Dieta Territorial las informaciones que, basadas en los datos almacenados, tales órganos o grupos exigieren dentro del marco de sus competencias, siempre que se dieren los supuestos previstos en el artículo 5, apartado 3, y existieren programas para su explotación.

2. Corresponde ejercer el derecho de información previsto en el apartado 1 del presente artículo, dentro del marco de las respectivas competencias, a los órganos representativos municipales y a las asambleas de corporaciones inframunicipales, así como a sus grupos parlamentarios y a los órganos correspondientes de las demás corporaciones e instituciones mencionadas en el artículo 1, frente a la Central de Tratamiento de Datos de Hesse, y los centros municipales de cálculo competentes, así como con respecto a cualesquiera otros sistemas de tratamiento de la información explotados por municipios y entidades inframunicipales. La solicitud de los grupos parlamentarios se elevará por conducto de la comisión permanente municipal.

3. En caso de duda, resolverá la autoridad de tutela.

Sección segunda

Del Interventor de Datos

ARTÍCULO 7

Situación jurídica

1. La Dieta Territorial elegirá, a propuesta del Gobierno del Estado, a un Interventor de Datos.

2. El Interventor de Datos estará ligado a la Administración por una relación de Derecho público, que se atemperará a lo dispuesto en la presente Ley. El cargo podrá ser encomendado asimismo a un funcionario a título de cargo accesorio, a un funcionario en situación de licencia o a un funcionario excedente.

3. El Interventor de Datos será elegido por la totalidad del período de la respectiva legislatura de la Dieta Territorial, permaneciendo en el desempeño del cargo hasta la nueva elección, una vez finalizada la legislatura. La reelección es admisible. Antes de expirar el período de su mandato, sólo podrá ser cesado si se dieren supuestos de hecho que, en caso de tratarse de un funcionario, justificaran la separación del servicio. Podrá en todo momento renunciar al cargo.

4. La retribución del Interventor de Datos será regulada mediante contrato.

Artículo 8

Independencia

No obstante las obligaciones que le competen en virtud de lo dispuesto en los artículos 10 y 12, el Interventor de Datos no estará sujeto a órdenes o instrucciones de órgano alguno.

Artículo 9

Deber de secreto

El Interventor de Datos estará obligado, aun después de la extinción de su relación de servicio, a guardar secreto sobre los asuntos de que hubiere tenido conocimiento en el ejercicio de su actividad oficial. Tal obligación no afectará a las comunicaciones producidas en el servicio ni a los hechos que fueren notorios o que, por su significación, no requirieren la observancia del secreto. Sin previa autorización no podrá formular declaración alguna, en juicio o fuera de él, acerca de asuntos sujetos al deber de secreto. Compete al Ministro Presidente conceder tal autorización.

Artículo 10

Funciones

1. El Interventor de Datos velará porque en el tratamiento mecánico de los datos por parte de las autoridades y entidades mencionadas en el artículo 1 sean observados los preceptos de la presente Ley

y cuantos otros preceptos hicieren referencia al trato confidencial de los datos de los ciudadanos y de los documentos concernientes a los ciudadanos individualmente considerados. Dará cuenta a la autoridad de tutela competente, de las violaciones que observare y propondrá medidas precautorias para el mejoramiento de la protección de datos.

2. El Interventor de Datos observará las repercusiones que el tratamiento mecánico de los datos tuviere sobre los métodos de trabajo y las competencias decisoras de las autoridades y entidades mencionadas en el artículo 1, determinando si tales repercusiones conducen a un desajuste en la división de los poderes entre los órganos constitucionales del Estado, entre los órganos de la Administración autónoma estatal y municipal, pudiendo suscitar medidas que estimare idóneas en orden a impedir tales repercusiones.

Artículo 11

Derecho de recurso

Toda persona tendrá derecho a acudir al Interventor de Datos si creyere ser lesionada en sus derechos por efecto del tratamiento de la información llevada a cabo por las autoridades y entidades mencionadas en el artículo 1.

Artículo 12

Investigaciones por cuenta de la Dieta Territorial y de los órganos de representación municipal

La Dieta Territorial, el Presidente de la Dieta Territorial, los grupos parlamentarios de la Dieta y los órganos de representación municipal mencionados en el artículo 6, apartado 2, podrán requerir que el Interventor de Datos investigue por qué razones no fueron contestadas, o fueron contestadas insuficientemente, las peticiones de información.

Artículo 13

Derecho de información

Las autoridades y entidades mencionadas en el artículo 1 deberán facilitar al Interventor de Datos las informaciones que el mismo precisare para el cumplimiento de sus funciones.

2. *Lel (sueca) de protección de datos* (DATALAG, *SFS 1973:289)*

DISPOSICIONES PRELIMINARES

ARTICULO 1

En la presente Ley se entenderá

— por *información personal,* la información que hiciere referencia a una persona física;
— por *archivo de personas,* el archivo, registro u otras anotaciones que se llevaren con ayuda del tratamiento automático de datos y que contuvieren información personal susceptible de ser relacionada con la persona a la que la información hiciere referencia;
— por *persona registrada,* la persona individual con relación a la cual existiere información personal en un archivo de personas;
— por *responsable del archivo,* la persona mediante cuya actividad se explotare el archivo de personas, si la misma dispusiere del archivo.

AUTORIZACION, ETC.

ARTÍCULO 2

No podrá ser creado o explotado un archivo de personas sin autorización de la Inspección de Datos.

El primer párrafo no será de aplicación en lo que respecta a los archivos de personas cuya creación fuere acordada por el Rey o la Dieta. Antes de la adopción del acuerdo deberá recabarse el dictamen de la Inspección de Datos.

ARTÍCULO 3

La Inspección de Datos concederá autorización para crear y explotar un archivo de personas si no existiere motivo alguno para creer que, con la debida observancia de las instrucciones dictadas de conformidad con lo dispuesto en los artículos 5 y 6, se hubiere de producir una intrusión indebida en la integridad personal de las personas registradas.

Para enjuiciar la posibilidad de que se produzca intrusión indebida en la integridad se prestará especial atención a la índole y cantidad

de las informaciones personales que debieren ser incluidas en el archivo, así como a la actitud que con respecto al archivo mostraren las personas físicas a registrar o a la actitud que fuere de esperar que muestren las mismas.

ARTÍCULO 4

La autorización para crear y explotar archivos de personas que contuvieren datos acerca de si una persona es sospechosa de delito, o ha sido sentenciada por delito o cumplido una pena o sufrido otra sanción por razón de delito, o ha sido objeto de medidas de seguridad previstas en la Ley de protección a la infancia (97/1960), en la Ley de temperancia (579/1954), en la Ley de prestación de tratamiento psiquiátrico aislado en casos determinados (293/1966), en la Ley sobre medidas a aplicar a ciertas personas afectadas de perturbaciones en el desarrollo psíquico (940/1967), en la Ley de medidas para casos de asocialidad socialmente peligrosa (450/1954) o en el estatuto de extranjería (Ley 193/1974), podrá ser concedida a persona distinta de la autoridad que, conforme a las Leyes o a otras disposiciones, hubiere de llevar registros de tales informaciones sólo si existiere una razón especial.

La autorización para crear o explotar un archivo de personas que contuvieren información acerca de enfermedades o estado de salud de alguien, o información acerca de si alguien ha recibido asistencia social, tratamiento de temperancia u otra información semejante, o acerca de si ha sido objeto de medidas con arreglo a la Ley de protección a la infancia o al estatuto de extranjería, podrá ser concedida a persona distinta de la autoridad que, conforme a las Leyes o a otras disposiciones, hubieren de llevar registros de tales informaciones sólo si existiere una razón especial.

La autorización para crear o explotar un archivo de personas que contuviere información acerca de la concepción política o religiosa de alguien sólo podrá ser concedida si existiere una razón especial. Lo que antecede no será de aplicación a los archivos de personas que una asociación considere conveniente crear con respecto a sus asociados.

ARTÍCULO 5

Cuando concediere autorización para crear y explotar un archivo de personas, la Inspección de Datos dictará instrucciones referentes a la finalidad del registro y a las informaciones que podrán incluirse en el mismo. Si existiere una razón especial, la autorización podrá ser limitada a un plazo determinado.

ARTÍCULO 6

Si fuere concedida la autorización para crear y explotar un archivo de personas, la Inspección de Datos, en tanto en cuanto fuere necesario para prevenir el riesgo de instrusión indebida en la integridad personal, dictará instrucciones acerca de los siguientes extremos:

1. Colecta de información para el archivo de personas.
2. Realización del tratamiento automático de la información.
3. Material técnico.
4. Tratamientos que hubieren de ser realizados automáticamente con las informaciones personales incluidas en el archivo.
5. Información a las personas afectadas.
6. Informaciones personales a las cuales se pudiere acceder.
7. Difusión de las informaciones personales y otras aplicaciones de las mismas.
8. Conservación y clasificación de las informaciones personales.
9. Control y seguridad.

Las instrucciones referentes a la difusión de información personal no podrán limitar las obligaciones que el ordenamiento de la libertad de imprenta atribuye a la autoridad competente.

ARTÍCULO 7

Las disposiciones de los artículos 5 y 6 referentes a la obligación de la Inspección de Datos de dictar instrucciones serán de aplicación asimismo en relación con los archivos de personas que se contemplan en el artículo 2, segundo párrafo, en tanto en cuanto ni el Rey ni la Dieta hubieran dictado instrucciones al respecto.

OBLIGACIONES DEL RESPONSABLE DEL ARCHIVO

ARTÍCULO 8

Si existiere motivo para sospechar que no es exacta la información personal registrada en un archivo de personas, el responsable del archivo adoptará sin demora medidas adecuadas para comprobar la exactitud de la información y, si hubiere razón para ello, la rectificará o la suprimirá del archivo.

Si la información rectificada o suprimida hubiere sido comunicada a persona distinta de la registrada, el responsable del registro deberá, si así lo solicitare la persona registrada, dar cuenta de la rectificación

o supresión a la persona a la cual tal información hubiera sido comunicada. Si hubiere una razón especial, la Inspección de Datos podrá eximir de tal obligación al responsable del archivo.

ARTÍCULO 9

Si un archivo de personas contuviere información personal que, habida cuenta de la finalidad del archivo, hubiere de considerarse incompleta, o si en un archivo de personas que comprendiere registros referentes a personas faltare algo que, habida cuenta de la finalidad del registro, fuere presumible que hubiera de estar registrado en el mismo, el responsable del archivo deberá proceder a completarlo según fuere necesario. Se procederá a completarlo en todo caso si hubiere motivo fundado para creer que la incompletud pudiera llevar consigo una intrusión indebida en la integridad personal o acarrear peligro de lesión de derechos.

ARTÍCULO 10

Si la solicitare la persona registrada, el responsable del archivo dará cuenta a la misma, tan pronto como fuere posible, de la información personal registrada en el archivo, indicando si contiene información referente a ella. Si tal información le hubiera sido ya facilitada, no será necesario facilitarla de nuevo a la misma persona registrada antes de que hubieren transcurrido doce meses.

La información prevista en el primer párrafo será facilitada sin gasto alguno para la persona registrada. Si hubiere una razón especial, la Inspección de Datos podrá disponer la exacción de una tasa en relación con determinadas clases de informaciones personales.

No será de aplicación el primer párrafo en el supuesto de que se tratare de información que, conforme a la Ley o a otras disposiciones, o de acuerdo con una resolución de la autoridad dictada al amparo de una disposición, no pudiere ser facilitada a la persona registrada.

ARTÍCULO 11

La información personal contenida en un archivo de personas no podrá ser difundida si hubiere motivo para creer que la información será empleada en un tratamiento automático de datos contrario a la presente Ley. Si hubiere motivo para creer que la información personal será empleada en un tratamiento automático de datos que tenga lugar en el extranjero, la información sólo podrá ser facilitada previa conformidad de la Inspección de Datos. Tal conformidad sólo podrá

ser prestada si pudiere admitirse que la facilitación de la información no lleva consigo una intrusión indebida en la integridad personal.

Por lo que respecta a la prohibición de que la autoridad comunique información, se hace remisión a las disposiciones que al efecto contiene la Ley de limitaciones al derecho de consultar documentos generales (249/1937).

ARTÍCULO 12

Si el responsable del archivo dejare de explotarlo, dará cuenta a la Inspección de Datos. La Inspección prescribirá en tal caso cómo deba procederse con el registro.

ARTÍCULO 13

El responsable del archivo o persona que se ocupare del archivo no podrá revelar a personas no autorizadas lo que como consecuencia de ello hubiere sabido acerca de las circunstancias personales de un individuo.

Si, de conformidad con instrucciones dictadas en virtud de lo dispuesto en los artículos 6 ó 18, fuere facilitada información personal en condiciones tales que restrinjan el derecho del receptor a difundir la información, el receptor o quien por cuenta suya se ocupare de aquélla, no podrá revelar a persona no autorizada lo que en tal forma hubiere sabido acerca de las circunstancias personales de un individuo.

ARTÍCULO 14

Si para instruir un proceso o expediente una autoridad hiciere uso de una grabación efectuada con miras al tratamiento automático de datos, la grabación será incorporada a la documentación del proceso o expediente en forma legible, a menos que razones especiales aconsejaren otra cosa.

INSPECCION, ETC.

ARTÍCULO 15

La Inspección de Datos velará porque el tratamiento automático de la información no ocasione intrusión indebida en la integridad personal.

Su función inspectora se ejercerá de tal manera que no ocasione gastos o molestias que excedan de lo necesario.

ARTÍCULO 16

La Inspección de Datos tendrá derecho, en orden al ejercicio de su función, a penetrar en los locales en los cuales se llevare a cabo el tratamiento automático de datos o estuvieren instalados la máquina o equipo, o se conservaren las grabaciones para el tratamiento automático de datos. La Inspección tendrá además derecho de acceso a los documentos que conciernen al tratamiento automático de la información y a modificar el uso de las máquinas de proceso de datos.

ARTÍCULO 17

El responsable del archivo facilitará a la Inspección de Datos aquellas informaciones que con respecto al tratamiento automático de los datos solicitare aquélla al objeto de llevar a cabo su función inspectora. La misma norma regirá con relación a quien explotare un archivo de personas por cuenta del responsable del archivo.

ARTÍCULO 18

Si la explotación de un archivo de personas condujere a una intrusión indebida en la integridad personal, o si hubiere motivo para creer que se haya de producir tal intrusión, la Inspección de Datos podrá, en la medida en que fuere necesario, modificar las instrucciones que con anterioridad hubieren sido dictadas o dictar nuevas instrucciones acerca de los extremos aludidos en los artículos 5 ó 6. Por lo que se refiere a los archivos contemplados en el segundo párrafo del artículo 2, la Inspección de Datos podrá adoptar las medidas aludidas sólo en tanto en cuanto no fueren contrarias a la resolución del Rey o de la Dieta.

Si no pudiere lograrse por otros medios la protección contra la intrusión indebida en la integridad personal, la Inspección de Datos podrá revocar la autorización concedida.

ARTÍCULO 19

El que en la Inspección de Datos se hubiere ocupado en expedientes relativos a las autorizaciones o inspecciones previstas en la presente Ley, no podrá revelar a personas no autorizadas aquello que hubiera llegado a conocer acerca de las circunstancias personales de un individuo o de secretos profesionales o comerciales.

SANCIONES PENALES E INDEMNIZACIONES DE DAÑOS Y PERJUICIOS, ETC.

Artículo 20

Será condenado a pena de multa o a privación de libertad de un año como máximo el que intencionadamente o por negligencia:

1. Creare o explotare archivos de personas sin la autorización prevista en la presente Ley, si tal autorización fuere preceptiva.
2. Infringiere las instrucciones dictadas de conformidad con los artículos 5, 6 ó 18.
3. Facilitare información personal en contra de lo dispuesto en el artículo 11.
4. Infringiere el artículo 12 o el 13.
5. Facilitare información falsa en el cumplimiento de la obligación de revelar información, prevista en el artículo 10.
6. Facilitare información falsa en el supuesto que se contempla en el artículo 17; o
7. Infringiere lo dispuesto en el artículo 19.

Sólo podrá ejercitarse la acción penal por razón de los delitos previstos en los artículos 13 ó 19, si el interesado formulare querella o si la acción penal procediere desde un punto de vista general.

Artículo 21

El que ilícitamente se proporcionare acceso a una grabación realizada con miras al tratamiento automático, o ilícitamente modificare o borrare, o introdujere en un archivo tal grabación, será condenado por intrusión a multa o a privación de libertad de dos años como máximo, a menos que la acción estuviere penada en el Código penal.

La tentativa o preparación del delito que se contempla en el primer párrafo será castigada a tenor de lo dispuesto en el capítulo 23 del Código penal. Si el delito hubiere sido consumado y resultare ser leve, no podrá ser castigado en los términos antedichos.

Artículo 22

Si se creare o explotare un archivo de personas sin la autorización prevista en la presente Ley, en los supuestos en que la misma fuere preceptiva, el archivo será declarado ilegal, a menos que ello resultare manifiestamente injusto.

ARTÍCULO 23

Si una persona registrada sufriere perjuicio por el hecho de que un archivo de personas contuviere información inexacta acerca de la misma, el responsable del archivo deberá indemnizarla. Para apreciar si se ha producido perjuicio y en qué medida se ha producido, se tendrán en cuenta la afección y otras circunstancias de significación distinta de la puramente económica.

ARTÍCULO 24

Si el responsable del archivo o el que por cuenta del mismo manejare un archivo de personas no facilitare el acceso al local o a los documentos en el supuesto contemplado en el artículo 16, o dejare de facilitar información a tenor de lo dispuesto en el artículo 17, la Inspección de Datos podrá imponer una multa. La misma norma regirá si el responsable del registro no cumpliere lo que le corresponda a tenor de los artículos 8, 9 ó 10.

ARTÍCULO 25

La acción para impugnar la resolución de la Inspección de Datos será ejercitada ante el Rey por medio de recurso de alzada. El Canciller de la Justicia podrá ejercitar la acción en defensa del interés general.

DISPOSICIONES TRANSITORIAS

La presente Ley entrará en vigor el 1 de julio de 1973. Lo dispuesto en los artículos 2 a 14 y 18, 20, apartados 1 a 5, 21 a 23 y 24, punto segundo, no entrará en vigor hasta el 1 de julio de 1974.

Sin perjuicio de lo dispuesto en el párrafo anterior, la Inspección de Datos podrá dictar instrucciones acerca de los extremos contemplados en los artículos 5 ó 6, antes del 1 de julio de 1974, si existieren razones especiales. Si alguien infringiere tales instrucciones, se aplicará lo dispuesto en el artículo 20, apartado 2, en materia de sanciones penales. La Inspección de Datos podrá asimismo con anterioridad a la fecha mencionada resolver peticiones de autorización y dictar instrucciones de conformidad con los artículos 5, 6 ó 18, en tanto en cuanto las mismas contemplaren el período de tiempo subsiguiente al transcurso del mes de junio de 1974.

Si un archivo de personas que según la Ley no pudiere ser explotado sin autorización estuviere en funcionamiento antes del 1 de julio de 1974, podrá ser explotado sin autorización hasta tanto la petición hubiere sido resuelta con carácter definitivo, siempre que la petición de autorización hubiera sido formulada antes del 1 de enero de 1975. La clase de información que comprendiere el archivo y la finalidad para la cual se empleare la información podrá ser modificada o ampliada previa solicitud formulada ante la Inspección de Datos. Si alguien infringiere lo dispuesto, se aplicarán las penas previstas en el artículo 20, apartado 1.

(Sigue la fórmula ejecutoria, fechada en el Palacio de Estocolmo a 11 de mayo de 1973, firma y sello del Rey y refrendo del Ministro de Justicia.)

3. *Ley de privacidad de 1974 (Estados Unidos).*

NOTA PRELIMINAR

El nombre completo del texto publicado en el «Federal Register» con la referencia «Public Law 93-579, 93rd Congress, S. 3418», promulgado el 31 de diciembre de 1974, es el siguiente: «Ley por la que se modifica el Título 5 del Código de los Estados Unidos, insertando una Sección 552a para salvaguardar la privacidad individual frente al uso indebido de los registros federales, disponer que los individuos tengan acceso a los registros que les conciernen, llevados por órganos federales; crear una Comisión de Estudio de la Protección a la Privacidad, y para otros fines.»

La Ley, citada oficialmente como «Privacy Act, 1974», comprende, además de la fórmula promulgatoria, un total de ocho «secciones», la primera de las cuales es la sección 2 y, correlativamente, comprende hasta la sección 9. La parte sustancial la constituye la sección 3, que añade una sección 552a a la 552 del título 5 del Código de los Estados Unidos. Este Código, o *United States Code*, constituye una compilación oficial de Leyes federales, distribuidas en 50 títulos, el primero de los cuales contiene las disposiciones generales, y los demás las normas reguladoras de materias diversas dispuestas por orden alfabético. Tanto la numeración de los títulos como la de las secciones de cada título dejan huecos, con el fin de añadir nuevos títulos o nuevas secciones. Concebido primitivamente (cuando se publicó su prime-

ra edición en 1926) como una compilación sin más valor normativo que el de una presunción *iuris tantum*, la mayor parte de los títulos (entre ellos el 5) fueron adoptados con valor de Leyes formales por el Congreso a partir de 1947.

La sección 2 de esta «Privacy Act, 1974», viene a ser una exposición de motivos, que contiene una explicación de los problemas para cuya solución se promulga la ley, así como una enumeración de las finalidades que se persiguen con tal promulgación.

El núcleo normativo básico lo constituye, como queda dicho, la sección 3, dividida en subsecciones identificadas con las letras (a) a (q). Las demás secciones comprenden las disposiciones finales, transitorias y de entrada en vigor. Entre ellas, la seción 5 crea una Comisión de Estudio de la Privacidad, de carácter temporal y que quedará disuelta *ipso iure* una vez redactado el informe para cuya preparación se crea.

TEXTO DE LA LEY DE PRIVACIDAD DE 1974

SECCION 2

(a) El Congreso estima que:

(1) La privacidad de un individuo es afectada directamente por la captación, conservación, uso y difusión de información personal por entes y órganos federales;

(2) el creciente uso de ordenadores y de una tecnología compleja de la información, si bien es esencial para el eficiente funcionamiento de las Administraciones públicas, ha aumentado grandemente el detrimento que para la privacidad individual puede derivarse de cualquier captación, conservación, uso y difusión de información personal;

(3) las posibilidades del individuo en cuanto a la seguridad en el empleo, a los beneficios de los seguros y al crédito, y su derecho a un proceso judicial y a otras formas de protección, son puestas en peligro por el abuso de ciertos sistemas de información;

(4) el derecho de privacidad es un derecho personal y fundamental protegido por la Constitución de los Estados Unidos, y

(5) para proteger la privacidad de individuos identificados en sistemas de información llevados por entes y órganos federales, es necesario y conveniente que el Congreso regule la captación, conservación, uso y difusión de información por tales entes y órganos.

(b) Finalidad de la presente ley es establecer determinadas medidas de protección del individuo contra la invasión de la privacidad personal exigiendo a los entes y órganos federales, que, salvo disposición legal en contrario:

(1) permitan al individuo decidir qué datos pertenecientes al mismo sean captados, conservados, usados o difundidos por tales entes u órganos;

(2) permitan al individuo impedir que los datos referentes al mismo, obtenidos por tales entes y órganos para una finalidad concreta, sean usados o puestos a disposición para otra finalidad sin su consentimiento;

(3) permitan al individuo tener acceso a información concerniente al mismo contenida en registros de entes y órganos federales, mandar sacar copia de la totalidad o parte de tales registros, y rectificarlos o enmendarlos;

(4) capten, conserven, usen o difundan cualquier registro de información personal, identificable, de manera que garantice que tal actuación se enderece a un fin necesario y legal, que la información es actual y precisa para el uso que se pretende, y que se han adoptado las medidas preventivas adecuadas para impedir el abuso de tal información;

(5) sólo permitan exenciones de los requisitos que con respecto a los registros se establecen en la presente ley en aquellos casos en que, según lo previsto al efecto en virtud de habilitación legal específica, existiere una necesidad importante de orden público que justificare tal exención; y

(6) respondan civilmente por cualesquiera daños y perjuicios que se produjeren como resultado de acción dolosa o intencionada que atentare contra los derechos del individuo reconocidos al amparo de la presente ley.

SECCION 3

Queda modificado el Título 5 del Código de los Estados Unidos con la adición a continuación de la sección 552 de la nueva sección siguiente:

«552a. *Registros llevados acerca de personas individuales.*

(a) DEFINICIONES. A los efectos de la presente sección:

(1) la voz «órgano» significará órgano tal como se define en la sección 552 (e) del presente Título;

(2) la voz «individuo» significará todo ciudadano de los Estados Unidos o extranjero legalmente autorizado para residir permanentemente;

(3) la voz «llevar» comprenderá la llevanza, agrupación, uso o difusión;

(4) la voz «registro» significará cualquier elemento, combinación o agrupación de información acerca de un individuo que fuere llevada por un órgano e incluyere, aunque no exclusivamente, información referente a su educación, sus operaciones financieras, historial médico. e historial penal o laboral, y contuviere su nombre, o el número o símbolo de identificación u otro detalle de identificación atribuido al individuo tal como una huella dactilar, grabación sonora o fotografía;

(5) la expresión «sistema de registros» significará un grupo de registros sujetos al control de un órgano, del cual se recuperare información a partir del nombre del individuo o de algún número o símbolo de identificación, o de otro detalle de identificación atribuido al individuo;

(6) la expresión «registro estadístico» significará un registro comprendido en un sistema de registros llevados a efectos de investigación o información estadística solamente y que no fuere usado, en todo o en parte, para adoptar una decisión acerca de un individuo identificable, sin perjuicio de lo dispuesto en la sección 8 del Título 13; y

(7) la expresión «uso de trámite» significará, con relación a la revelación de un registro, el uso del registro para una finalidad compatible con la finalidad para la cual hubiera sido obtenido.

(b) Requisitos de la Revelación. Ningún órgano revelará registro alguno que estuviere contenido en un sistema de registros, por ningún medio de comunicación, a ninguna persona, ni a otro órgano, excepto en virtud de petición formulada por escrito por el individuo al cual perteneciere el registro o con el previo consentimiento escrito de dicho individuo, a menos que la revelación del registro fuere hecha:

(1) a los directivos y empleados del órgano que llevare el registro, que para el cumplimiento de sus deberes tuvieren necesidad del registro;

(2) en virtud de la sección 552 del presente Título;

(3) para usos de trámite, tal como los mismos se definen en la subsección (a) (7) de la presente sección y se detallan en la subsección (e) (4) (D) de la presente sección;

(4) a la Oficina del Censo con miras a la preparación o la realización de un censo o encuesta u otra actividad de acuerdo con las disposiciones del Título 13;

(5) a una persona que hubiera facilitado previamente al órgano un adecuado compromiso escrito de que el registro será usado solamente como un dato de investigación o información estadística y de que el registro será transferido en forma no identificable con respecto a un individuo;

(6) a los Archivos Nacionales de los Estados Unidos en cuanto registro dotado de valor histórico o de otra índole, suficiente para justificar su conservación continuada por la Administración de los Estados Unidos, o para su valoración, bien por el Administrador de Servicios Generales, bien por la persona que el mismo designare, para determinar si el registro tiene tal valor;

(7) a otro órgano o a un ente dependiente de un órgano de los Estados Unidos o sujeto al control de los Estados Unidos, con miras a una actividad de aplicación de las leyes civiles o penales, si tal actividad estuviere autorizada por disposición legal, y si el titular del órgano o ente hubiera formulado una petición escrita al órgano que llevare el registro en la cual se especificaren la parte concreta deseada y la actividad de aplicación de las leyes para la cual se requiriere el registro;

(8) a una persona, si se probare la existencia de circunstancias poderosas que afectaren a la salud o a la seguridad de un individuo, siempre que, una vez hecha la revelación, se comunicare a la última dirección conocida de dicho individuo;

(9) a una de las Cámaras del Congreso o, en la medida en que se tratare de asuntos de su competencia, a cualquier comité o subcomité de la misma, a cualquier comité conjunto del Congreso o subcomité de dicho comité conjunto;

(10) al Interventor General o a alguno de sus delegados, en el ejercicio de las funciones propias de la Oficina General de Contabilidad; o

(11) en virtud de mandamiento librado por tribunal competente.

(c) CONTABILIDAD DE DETERMINADAS REVELACIONES DE REGISTROS. En relación con cada sistema de registros sujeto a su control, cada órgano deberá:

(1) excepto por lo que respecta a las revelaciones de registros hechas al amparo de las subsecciones **(b)** (1) o **(b)** (2) de la presente sección, llevar una contabilidad exacta de:

(A) la fecha, naturaleza, y finalidad de cada revelación de un registro hecha a cualquier persona o a otro órgano al amparo de la subsección **(b)** de la presente sección; y

(B) el nombre y dirección de la persona u órgano a quien se hiciere la revelación;

(2) conservar la contabilidad realizada en virtud del parágrafo (1) de la presente subsección por espacio de cinco años por lo menos o durante la vida del registro, debiendo tomarse al respecto aquel de dichos dos períodos de tiempo que fuere más largo, a partir de la revelación de la cual se hiciere la contabilidad;

(3) excepto por lo que respecta a las revelaciones de registros hechas al amparo de la subsección **(b)** (7) de la presente sección, poner la contabilidad realizada en virtud del parágrafo (1) de la presente subsección a disposición del individuo mencionado en el registro, si así lo solicitare éste; e

(4) informar a cualquier persona o a otro órgano de cualquier corrección o anotación referente a litigios o controversias, que hubiera sido llevada a cabo por el órgano de conformidad con lo dispuesto en la subsección **(d)** de la presente sección en un registro que hubiere sido revelado a dicha persona, órgano, si se hubiera contabilizado la revelación.

(d) Acceso a los registros. El órgano que llevare un sistema de registros deberá:

(1) previa petición de un individuo, de acceder a su registro o a cualquier información que, haciendo referencia a su persona, estuviera contenida en el sistema, permitir a dicho individuo y, a instancia de éste, a la persona que el mismo eligiere para que le acompañare, examinar el registro y mandar hacer una copia de la totalidad o de cualquier parte del mismo en forma comprensible para él; pudiendo, no obstante, el órgano exigir a dicho individuo que aporte una declaración escrita por la cual se autorice que el registro del individuo sea objeto de examen y deliberación en presencia de la persona acompañante;

(2) permitir al individuo que solicite la modificación de un registro que hiciere referencia a su persona, y

(A) dentro de un plazo que no excediere de diez días (excluidos sábados, domingos y fiestas oficiales) a partir de la fecha de recepción de la petición hecha al efecto, acusar recibo de ésta por escrito; y

(B) proceder puntualmente.

(i) bien a efectuar cualquier corrección de cualquier parte del mismo que el individuo creyere que no es exacta, relevante, oportuna o completa;

(ii) bien a informar al individuo de su negativa a modificar el registro de conformidad con su solicitud, de la razón de la negativa, de los trámites prescritos por el órgano para que el individuo solicite la revisión de tal negativa por el titular del órgano o por un directivo designado por el titular del órgano, así como del nombre y dirección oficial de dicho funcionario;

(3) permitir al individuo que no estuviere de acuerdo con la negativa del órgano a modificar su registro, que solicite la revisión de tal negativa y que dentro de un plazo que no exceda de treinta días (excluidos sábados, domingos y fiestas públicas oficiales) a contar de la fecha en que el individuo hubiera solicitado la revisión, ultimar tal revisión y dictar una resolución definitiva, a menos que, existiendo justa causa probada, el titular del órgano prorrogare dicho plazo de treinta días; y si, después de la revisión, el funcionario revisor se negare asimismo a modificar el registro de acuerdo con lo solicitado, permitir al individuo que presente al órgano una breve declaración en la cual exponga las razones de su disconformidad con la negativa del órgano, e instruir al individuo de las disposiciones aplicables a la revisión en vía judicial de la resolución dictada por el funcionario revisor al amparo de lo dispuesto en la subsección (g) (1) (A) de la presente sección;

(4) en cualquier revelación que contuviere información acerca de la cual el individuo hubiera presentado declaración de disconformidad, y que se hubiere producido después de la presentación de la declaración prevista en el parágrafo (3) de la presente subsección, tomar buena nota de la parte del registro que fuere objeto de controversia y facilitar a las personas o a otros órganos a quienes hubiera sido revelado el registro controvertido copias de la aludida declaración y, si el órgano lo estimare oportuno, copias de una declaración concisa de las razones que hubiera tenido el órgano para no llevar a cabo las modificaciones interesadas.

(5) Nada de lo dispuesto en la presente sección permitirá a individuo alguno acceder a ninguna información recopilada con una antelación razonable con respecto a un pleito civil o expediente.

(e) Requisitos que deben cumplir los Organos. Todo órgano que llevare un sistema de registros deberá:

(1) conservar en sus registros solamente aquella información referente a individuos que fuere relevante y necesaria para realizar un fin que en virtud de disposición legal o decreto presidencial hubiere de ser realizado por el órgano;

(2) recoger información a ser posible directamente del individuo

interesado, cuando la información pudiere dar lugar a resoluciones adversas acerca de los derechos, beneficios y privilegios del individuo en aplicación de programas federales;

(3) informar a cada individuo al cual requiriere a que facilitare información, bien en el formulario que utilizare para la recogida de la información, bien en un formulario separado que podrá ser conservado por el individuo.

(A) de la autorización (concedida por disposición legal o por decreto presidencial) que permitiere solicitar la información, y de si la revelación de tal información es obligatoria o voluntaria;

(B) de la finalidad o finalidades principales para las cuales se pretende usar la información;

(C) de los usos de trámite que pudieren hacerse de la información publicada en virtud del parágrafo (4) (I) de la presente subsección; y

(D) de las consecuencias que, en su caso, le producirá el no facilitar todo o parte de la información;

(4) sin perjuicio de las disposiciones del parágrafo (11) de la presente subsección, publicar en el Registro Federal, anualmente por lo menos, una nota acerca de la existencia y carácter del sistema de registros, que comprenderá:

(A) el nombre y localización del sistema;

(B) las clases de individuos acerca de los cuales se llevaren registros en el sistema;

(C) las clases de registros llevados en el sistema;

(D) cada uso de trámite de los registros contenidos en el sistema, comprendidos los grupos de usuarios y la finalidad de tal uso;

(E) los criterios y prácticas del órgano con respecto al almacenamiento, la recuperabilidad de los registros, los controles del acceso a los mismos, su retención y la disposición sobre los mismos;

(F) la denominación del cargo y la dirección oficial del funcionario del órgano, responsable del sistema de registros;

(G) los trámites previstos por el órgano para notificar al interesado, a su instancia, si el sistema de registros contiene un registro referente al mismo;

(H) los trámites previstos por el órgano para comunicar al interesado, a su instancia, el modo en que pudiere tener acceso a cualquier registro referente al mismo, contenido en el sistema de registros y la forma de impugnar su contenido; e

(I) las clases de fuentes de los registros del sistema;

(5) llevar todos aquellos registros que el órgano utilizare para adoptar cualquier resolución acerca de cualquier individuo, con la

exactitud, relevancia, oportunidad y completud que razonablemente fueren necesarias para asegurar la imparcialidad de la resolución para con el individuo;

(6) antes de comunicar un registro referente a un individuo a una persona que no fuere un órgano, y a menos que la comunicación fuere hecha en virtud de la subsección (b) (2) de la presente sección, hacer cuanto fuere razonable para garantizar que tales registros son exactos, completos, oportunos y relevantes para los fines del órgano;

(7) no llevar registro alguno que detallare el modo en que un individuo ejerce derechos garantizados por la Primera Enmienda, a menos que estuviere expresamente autorizado por disposición legal o por el individuo al cual hiciere referencia el registro, o a menos que fuere pertinente para una actividad autorizada de aplicación de las leyes, o estuviere comprendida dentro del ámbito de tal actividad;

(8) hacer cuanto fuere necesario para dar cuenta a un individuo cuando el registro referente a dicho individuo fuere puesto a disposición de una persona en razón de mandamiento judicial que fuere de interés público;

(9) formular normas deontológicas para las personas ocupadas en la concepción, desarrollo, explotación o actualización de un sistema de registros, o en la llevanza de registros, e informar a tales personas con respecto a las reglas y condiciones de la presente sección, comprendidas cualesquiera otras reglas y trámites prescritos en virtud de la presente sección, así como las sanciones por incumplimiento;

(10) establecer las medidas precautorias, administrativas, técnicas y físicas adecuadas para garantizar la seguridad y confidencialidad de los registros y para protegerlos contra cualesquiera previsibles amenazas o azares contra su seguridad o integridad, que pudieren dar lugar a daños, dificultades, molestias o desigualdades de importancia para un individuo sobre el cual fuere llevada información; y

(11) por lo menos treinta días antes de la publicación o información prescrita en el parágrafo (4) (D) de la presente subsección, publicar en el Registro Federal el aviso de cualquier nuevo uso o uso previsto de la información contenida en el sistema, y dar a las personas interesadas ocasión de facilitar al órgano datos, opiniones o alegaciones por escrito.

(f) Disposiciones reglamentarias del Organo. Para ejecutar lo dispuesto en la presente sección, cada órgano que llevare un sistema de registros dictará disposiciones reglamentarias que, de conformidad con los requisitos prescritos en la sección 553 del presente título (incluida la información pública) deberán:

(1) prever trámites por los cuales pueda comunicarse al individuo, en respuesta a su solicitud, si un sistema de registros referidos a individuos contiene un registro concerniente al mismo;

(2) fijar unos momentos, lugares y requisitos razonables para identificar al individuo que solicitare su registro o la información referente al mismo antes de que el órgano pusiere el registro o la información a disposición del individuo;

(3) prever trámites para revelar al individuo, a su instancia, su registro o la información concerniente al mismo, inclusive un procedimiento especial, si se considerare necesario para revelar al interesado registros médicos, comprendidos los psicológicos, concernientes al mismo;

(4) prever trámites para conocer de la solicitud de un individuo referente a la modificación de un registro o de información concerniente al mismo, para formular una resolución acerca de la solicitud, para recurrir ante el órgano contra una resolución inicial adversa, y para cualesquiera medios adicionales que fueren necesarios para que cada individuo pudiere ejercer plenamente los derechos que le corresponden al amparo de la presente sección; y

(5) fijar las tasas que hubieren de ser exigidas, en su caso, a un individuo por hacer copias de su registro, sin perjuicio del coste de la búsqueda y examen del registro.

La Oficina del Registro Federal compilará y publicará anualmente las disposiciones reglamentarias promulgadas al amparo de la presente subsección y los avisos de los órganos, publicados al amparo de la subsección **(e)** (4) de la presente sección, en forma accesible al público a bajo coste.

(g) (1) REMEDIOS EN VÍA CIVIL. Siempre que un órgano:

(A) resolviere, al amparo de la subsección **(d)** (3) de la presente sección, no modificar el registro de un individuo de conformidad con su petición o no procediere a la revisión prescrita en dicha subsección;

(B) se negare a cumplir una petición individual formulada al amparo de la subsección **(d)** (1) de la presente sección;

(C) no llevare un registro concerniente a un individuo con la exactitud, relevancia, oportunidad y completud que fueren necesarias para asegurar la imparcialidad en cualquier resolución que, con respecto a las condiciones de aptitud, personalidad, derechos, oportunidades o beneficios de un individuo, pudiere ser dictada sobre la base de tal registro y, como consecuencia de ello, se dictare una resolución adversa para el individuo; o

(D) incumpliere cualquier otra disposición de la presente sección, o cualquier disposición reglamentaria promulgada al amparo de la misma, de tal manera que produjere efectos adversos para un individuo.

El individuo podrá deducir demanda en vía civil contra el órgano, siendo competentes los tribunales de distrito de los Estados Unidos para conocer de los asuntos comprendidos dentro del ámbito de las disposiciones de la presente subsección.

(2) (A) En toda causa instada al amparo de las disposiciones de la subsección (g) (1) (A) de la presente sección, el tribunal podrá ordenar al órgano que modifique el registro del individuo de conformidad con su petición o en la forma que el tribunal ordenare. En tal supuesto el tribunal resolverá el asunto *de novo*.

(B) El tribunal podrá liquidar contra los Estados Unidos unos honorarios razonables de letrado y otras costas irrogadas razonablemente en cualquier supuesto comprendido en el ámbito del presente parágrafo en el cual se hubieren estimado sustancialmente las peticiones del demandante.

(3) (A) En toda causa instada al amparo de las disposiciones de la subsección (g) (1) (B) de la presente sección, el tribunal podrá prohibir al órgano que oculte los registros y ordenarle exhiba al demandante cualesquiera registros referentes al mismo y que le hubieran sido ocultados indebidamente. En tal supuesto el tribunal resolverá el asunto *de novo*, y podrá examinar a puerta cerrada el contenido de los registros de cualquier órgano para resolver sobre si los registros o cualquier parte de los mismos pueden ser ocultados al amparo de alguna de las exenciones indicadas en la subesección (K) de la presente sección, correspondiendo al órgano la carga de apoyar su alegato al efecto.

(B) El tribunal podrá liquidar contra los Estados Unidos unos honorarios razonables de letrado y otras costas irrogadas razonablemente en cualquier supuesto comprendido dentro del ámbito del presente parágrafo en el cual se hubieren estimado sustancialmente las peticiones del demandante.

(4) En toda causa instada al amparo de las disposiciones de la subsección (g) (1) (C) o (D) de la presente sección, en la cual el tribunal resolviere que el órgano había actuado de manera intencionada, los Estados Unidos responderán ante el individuo por un importe igual a la suma de:

(A) los perjuicios efectivos sufridos por el individuo como resultado de la negativa u omisión, si bien en ningún caso percibirá la

persona con derecho a indemnización una suma inferior a 1.000 dólares; y

(B) las costas del proceso, juntamente con unos honorarios razonables de letrado tasados por el tribunal.

(5) La demanda para exigir el cumplimiento de una obligación creada al amparo de la presente sección podrá ser deducida ante el tribunal de distrito de los Estados Unidos que fuere competente en el distrito en el cual el demandante residiere o tuviere su centro principal de actividad mercantil, o en el que radicaren los registros del órgano, o bien en el Distrito de Columbia, cualquiera que fuere la cantidad objeto de controversia, dentro del plazo de dos años subsiguientes a la fecha en la cual se produjeren los hechos que dieren lugar a la demanda. No obstante, si un órgano hubiere falseado sustancial e intencionadamente una información que en virtud de la presente sección hubiere de ser revelada a un individuo, y la información falseada fuere importante para determinar la responsabilidad que en virtud de la presente sección correspondiere al órgano para con el individuo, la demanda podrá ser deducida en cualquier momento dentro de los dos años subsiguientes al descubrimiento de la falsedad por el individuo. Nada de lo contenido en la presente sección será interpretado en el sentido de autorizar una demanda civil por razón de perjuicios sufridos como resultado de la revelación de un registro hecha antes de la fecha de entrada en vigor de la presente sección.

(h) Derechos de los Tutores Legítimos. A los efectos de la presente sección, el padre o madre de un menor, o el tutor legítimo de un individuo que hubiere sido declarado incapaz por razón de defecto físico o mental o por razón de edad por tribunal competente, podrá actuar en nombre de dicho individuo.

(i) (1) Sanciones Penales. El directivo o empleado de un órgano que, en razón de su empleo o cargo, tuviere en su poder registros de dicho órgano que contuvieren información identificable con respecto a un individuo y cuya revelación estuviere prohibida por la presente sección o por disposiciones reglamentarias dictadas al amparo de la misma, o que, en razón de tal empleo o cargo, tuviere acceso a tales registros, y que, a sabiendas de que la revelación de tal material está prohibida, revelare dolosamente la información, de cualquier manera, a cualquier persona u órgano que no tuviere derecho a recibirla, será culpable de delito leve y castigado con multa que no excederá de 5.000 dólares.

(2) El directivo o empleado de un órgano que dolosamente llevare

un sistema de registros sin cumplir los requisitos de publicidad prescritos en la subsección (e) (4) de la presente sección, será culpable de delito leve y castigado con multa que no excederá de 5.000 dólares.

(3) La persona que, a sabiendas y dolosamente requiriere u obtuviere de un órgano, aduciendo razones falsas, un registro concerniente a un individuo, será culpable de delito leve y castigado con multa que no excederá de 5.000 dólares.

(j) Exenciones Generales. El titular de cualquier órgano podrá dictar disposiciones reglamentarias, de conformidad con los requisitos (incluido el de información pública) prescritos al efecto en las secciones 553 (b) (1), (2) y (3), (c) y (e) del presente título, para eximir a cualquier sistema de registros del órgano, de cualquier parte de la presente sección, excepto las subsecciones (b), (c) (1) y (2), (e) (4) (A) a (F), (e) (b), (7), (9), (10) y (11) e (i), si el sistema de registros:

(1) fuere llevado por la Agencia Central de Información; o

(2) fuere llevado por un órgano o por una unidad de un órgano que, como función principal, realizare alguna actividad que hiciere referencia a la aplicación de las leyes penales, entendiéndose comprendidos en tales actividades los esfuerzos desplegados por la policía para prevenir, dominar o reducir el delito o para aprehender a los delincuentes, así como las actividades de los fiscales, tribunales, autoridades correccionales, autoridades competentes en materia de libertad vigilada, remisión de penas, libertad bajo palabra, y que consistieren en (A) información recopilada con miras a identificar delicuentes y delincuentes presuntos, y constituida sólo por datos de identificación, y anotaciones de detenciones, naturaleza y estructura de las acusaciones, sentencias, confinamiento, puesta en libertad, situación de libertad bajo palabra y de libertad vigilada; (B) información recopilada a efectos de una investigación criminal, comprendidos atestados e informes, y vinculada a un individuo, recopilados en cualquier estadio del proceso de aplicación de las leyes penales, desde la detención o procesamiento hasta la supresión de toda vigilancia.

En el momento en que fueren dictadas las disposiciones reglamentarias previstas en la presente sección, el órgano incluirá en la memoria prescrita por la sección 553 (c) del presente título las razones por las cuales el sistema de registros hubiere de ser eximido de una disposición de la presente sección.

(k) Exenciones Específicas. El titular de un órgano podrá dictar disposiciones reglamentarias, de conformidad con los requisitos (inclusive la información pública) prescritos en las secciones 553 (b) (1), (2) y (3), (c) y (e) del presente Título, para eximir a cualquier sistema

de registros del órgano de la aplicación de las subsecciones (c) (3), (d), (e) (1), (e) (4) (G), (H) e (I) y (f) de la presente sección, siempre que el sistema de registros:

(1) estuviere sujeto a las disposiciones de la sección 552 (b) (1) del presente Título;

(2) constituyere material sujeto a investigación, recopilado con fines policiales, y no fuere material comprendido dentro del ámbito de aplicación de la subsección (j) (2) de la presente sección; si bien en el supuesto de que se denegare a un individuo un derecho, privilegio, o beneficio, que en caso contrario le correspondería en virtud de disposición legal federal o para el cual reuniere en caso contrario las condiciones necesarias, y tal denegación fuere resultado de la llevanza de tales registros, dichos registros serán facilitados a dicho individuo, excepto en la medida en que la revelación mostrare la identidad de una fuente que hubiere proporcionado información a la Administración bajo promesa expresa de que la identidad de la fuente sería mantenida en secreto o, antes de la fecha de entrada en vigor de la presente sección, bajo la promesa presunta de que la identidad de la fuente sería mantenida en secreto;

(3) fuere llevado en relación con la prestación de servicios de protección al presidente de los Estados Unidos u otros individuos a tenor de lo dispuesto en la sección 3056 del Título 18;

(4) hubiere de ser llevado y utilizado solamente como sistema de registros estadísticos en virtud de disposición legal;

(5) constituyere material sujeto a investigación recopilado solamente con el fin de determinar la aptitud, elegibilidad, o condiciones para el empleo civil federal, el servicio militar, los contratos federales, o el acceso a la información clasificada, pero sólo en la medida en que la revelación de tal material mostrare la identidad de una fuente que hubiera facilitado información a la Administración bajo promesa expresa de que la identidad de la fuente sería mantenida en secreto o, antes de la entrada en vigor de la presente sección, bajo promesa presunta de que la identidad de la fuente sería matenida en secreto;

(6) constituyere material de exámenes utilizado solamente para determinar las condiciones individuales necesarias para el nombramiento o el ascenso en la función pública federal, y su revelación comprometería la objetividad o pureza del procedimiento de examen; o

(7) constituyere material de evaluación utilizado para determinar las posibilidades de ascenso en las fuerzas armadas, pero sólo en la medida en que la revelación de tal material mostrare la identidad de

una fuente que hubiere facilitado información a la Administración bajo promesa expresa de que la identidad de la fuente sería mantenida en secreto o, antes de la fecha de entrada en vigor de la presente sección, bajo promesa presunta de que la identidad de la fuente sería mantenida en secreto.

En el momento en que fueren dictadas las disposiciones reglamentarias al amparo de la presente subsección, el órgano incluirá en la memoria prescrita en la sección 553 (c) del presente Título, las razones por las cuales el sistema de registros hubiere de ser eximido de una disposición de la presente sección.

(l) (1) Registros de Archivo. Cada registro de un órgano que fuere aceptado por el Administrador de Servicios Generales para su almacenamiento, tratamiento y servicio de conformidad con la sección 3103 del Título 44, se considerará, a los efectos de la presente sección, que es llevado por el órgano que hubiere depositado el registro y estará sujeto a las disposiciones de la presente sección. El Administrador de Servicios Generales no revelará el registro excepto al órgano que llevare el registro, o ajustándose a disposiciones reglamentarias dictadas por el órgano y que no fueren incompatibles con las disposiciones de la presente sección.

(2) Cada registro de un órgano, perteneciente a un individuo identificable, que hubiere sido transferido a los Archivos Nacionales de los Estados Unidos como un registro dotado de valor histórico o de otra índole, suficiente para justificar su conservación continuada por la Administración de los Estados Unidos antes de la fecha de entrada en vigor de la presente sección, se considerará, a los efectos de la presente sección, que es llevado por los Archivos Nacionales y no estará sujeto a las disposiciones de la presente sección, si bien deberá publicarse en el Registro Federal una memoria en la cual se describan de modo general tales registros (de acuerdo con los requisitos prescritos con respecto a los registros sujetos a las subsecciones (e) (4) (A) a (G) de la presente sección).

(3) Cada registro de un órgano, perteneciente a un individuo identificable, que hubiere sido transferido a los Archivos Nacionales de los Estados Unidos como un registro dotado de valor histórico o de otra índole, suficiente para justificar su conservación continuada por la Administración de los Estados Unidos en la fecha de entrada en vigor de la presente sección o con posterioridad a dicha fecha, se considerará, a los efectos de la presente sección, que es llevado por los Archivos Nacionales y estará exento de los requisitos prescritos por la sección, excepto los de las subvenciones (e) (4) (A) a (G) y (e) (9) de la presente sección.

(m) CONTRATISTAS PÚBLICOS. Cuando un órgano contratare la explotación por el órgano o en su nombre, de un sistema de registros, con miras a cumplir una función del órgano, el órgano dispondrá, de conformidad con su competencia, que las prescripciones de la presente sección sean aplicadas a dicho sistema. A los efectos prevenidos en la subsección (i) de la presente sección el contratista y cualquier empleado del contratista serán considerados empleados del órgano, si el contrato hubiera sido concertado en la fecha de entrada en vigor de la presente sección o con posterioridad a dicha fecha.

(n) LISTAS DE ENVÍOS POSTALES. El nombre y dirección de un individuo no podrá ser vendido o alquilado por un órgano, a menos que tal acto estuviere específicamente autorizado por la ley. Esta disposición no será interpretada en el sentido de exigir la ocultación de nombres y direcciones cuya publicidad estuviere permitida a otros efectos.

(o) DENUNCIA DE NUEVOS SISTEMAS. Todo órgano dará cuenta anticipadamente al Congreso y a la Oficina de Dirección y Presupuesto, de cualquier propuesta de creación o modificación de cualquier sistema de registros, al objeto de hacer posible una valoración de la repercusión probable o potencial de tal propuesta sobre la privacidad y otros derechos personales o reales de los individuos, o de la revelación de la información referente a tales individuos, y su repercusión sobre la preservación de los principios constitucionales de federalismo y separación de poderes.

(p) MEMORIA ANUAL. El Presidente elevará al Presidente de la Cámara y al Presidente del Senado, el 30 de junio de cada año natural, una memoria de conjunto, en la que se relacionarán por separado el número de registros contenidos en cualquier sistema de registros que hubieran estado exentos de la aplicación de las subsecciones (j) y (k) de la presente sección durante el año natural precedente, y las razones de las exenciones, así como cualquier otra información que revelare el esfuerzo por aplicar plenamente la presente sección.

(q) EFECTOS SOBRE OTRAS LEYES. Ningún órgano se apoyará en exención alguna contenida en la sección 552 del presente título para ocultar a un individuo un registro que de otro modo fuere accesible a dicho individuo al amparo de las disposiciones de la presente sección.»

SECCION 4

La subdivisión del capítulo 5 del título 5 del Código de los Estados Unidos queda modificada por la inserción del epígrafe:

«552a. Registros acerca de personas individuales»

a continuación del epígrafe:

«552. Información pública; reglamentos, dictámenes, resoluciones y procedimientos de los órganos.»

SECCION 5

(a) (1) Se crea una Comisión de Estudio de la Protección de la Privacidad (aludida en lo que sigue como la «Comisión»), que estará compuesta por siete miembros, de conformidad con lo que se indica a continuación:

(A) tres designados por el Presidente de los Estados Unidos;

(B) tres designados por el Presidente del Senado;

(C) dos designados por el Presidente de la Cámara de Representantes.

Los miembros de la Comisión serán seleccionados entre personas que, en razón de los conocimientos y pericia que poseyeren en alguno de los siguientes ámbitos: derechos fundamentales y libertades públicas, Derecho, ciencias sociales, tecnología de ordenadores, dirección de empresas, administración de archivos y administración pública estatal y municipal, reunieren condiciones para prestar servicio en la Comisión.

(2) Los miembros de la Comisión elegirán de su seno a un presidente.

(3) La producción de una vacante en la composición de la Comisión no suspenderá las facultades de la Comisión, en tanto en cuanto hubiere cuatro miembros en ejercicio activo, si bien la vacante deberá ser cubierta de la misma manera que fuera llevada a cabo la primitiva designación.

(4) El quórum de válida constitución de la Comisión lo formará la mayoría de sus miembros, si bien la Comisión podrá señalar un número inferior de miembros como quórum a efectos de recibir declaraciones. La Comisión estará autorizada para crear los comités que fueren necesarios para el desempeño de sus funciones y para delegar en los mismos aquellas facultades que fueren precisas al efecto. Cada miembro de la Comisión, incluido el presidente, tendrá las mismas obligaciones y facultades en todas las decisiones y actos

de la Comisión; gozará de pleno acceso a toda la información necesaria para el ejercicio de sus funciones, y tendrá un voto. Los actos de la Comisión requerirán el voto mayoritario de los miembros presentes. El presidente (o el miembro designado por el presidente como presidente en funciones) será el portavoz oficial de la Comisión en sus relaciones con el Congreso, con los órganos de la Administración, otras personas y el público, y, en representación de la Comisión, velará por la fiel ejecución de los criterios administrativos y las decisiones de la Comisión, informando al respecto a la Comisión cuando procediere o según ordenare la Comisión.

(5) (A) Siempre que la Comisión elevare un presupuesto de gastos o una petición al Presidente de la Oficina de Dirección y Presupuesto, remitirá simultáneamente al Congreso una copia de tal petición.

(B) Siempre que la Comisión elevare al Presidente de la Oficina de Dirección y Presupuesto recomendaciones legislativas, informes o comentarios sobre legislación, remitirá simultáneamente al Congreso copia de tales recomendaciones, informes o comentarios. Ningún funcionario u órgano de los Estados Unidos tendrá facultad para requerir a la Comisión a que eleve sus recomendaciones legislativas, informes o comentarios de legislación a ningún funcionario u órgano de los Estados Unidos, para su aprobación, comentario o examen, antes de que tales recomendaciones, informes o comentarios hubieren sido elevados al Congreso.

(b) La Comisión procederá

(1) a realizar un estudio de los bancos de datos, programas de tratamiento automático de datos, y sistemas de información de organizaciones de la Administración, entidades regionales y privadas, con miras a determinar los criterios y métodos en vigor en materia de protección de la información personal; y

(2) a recomendar al Presidente del Congreso la extensión en que, en su caso, los requisitos y principios de la sección 552a del título 5 del Código de los Estados Unidos debiere ser aplicada a las prácticas informáticas de tales organizaciones, mediante legislación, actuación administrativa o adopción voluntaria de tales requisitos y principios; y a informar sobre las demás recomendaciones legislativas que considerare necesarias para proteger la privacidad de los individuos, satisfaciendo a la vez las necesidades de información del Estado y la sociedad.

(c) (1) Al realizar el estudio prescrito por la subsección **(b)** (1) de la presente sección, y en los informes que evacuare al respecto, la Comisión podrá investigar, examinar y analizar

(A) la transferencia interestatal de información sobre individuos,

efectuada a través de archivos manuales o por ordenador u otros medios electrónicos o de telecomunicación;

(B) los bancos de datos y programas y sistemas de información cuyo funcionamiento afectare de manera significativa o sustancial al goce del derecho de privacidad y de otros derechos personales y reales de los individuos;

(C) el uso de números de la seguridad social, números de placas de licencia, identificadores universales y otros símbolos, para identificar a los individuos registrados en los bancos de datos y para acceder a los sistemas de información y archivos, así como para integrarlos o centralizarlos; y

(D) la comprobación y análisis de datos estadísticos, tales como los datos del censo federal, con otras fuentes de datos personales, tales como registros de automóviles y guías telefónicas, con miras a reconstruir las respuestas individuales dadas a los cuestionarios estadísticos destinados a fines comerciales o de otra índole, de tal manera que dieren lugar a una violación de la confidencialidad presunta o expresa de tal información.

(2) (A) La Comisión podrá incluir en su examen actividades de información personal referidas a los siguientes ámbitos: medicina, seguros, educación, empleo y personal, crédito, instituciones bancarias y financieras, oficinas de crédito, la industria de información comercial, televisión por cable y otros medios de telecomunicación, reservas turísticas, hoteleras y de espectáculos, y tratamiento electrónico de cheques.

(B) La Comisión incluirá en su examen un estudio referente a los extremos siguientes:

(i) si una persona ocupada en el comercio interestatal, que llevare una lista de envíos postales debería ser requerida a suprimir de dicha lista el nombre y dirección de un individuo a instancia de dicho individuo;

(ii) si debería prohibirse al Servicio de la Renta Interior transferir a otros órganos y a órganos de las Administraciones estatales datos identificables con referencia a individuos;

(iii) si la Administración federal debería indemnizar los perjuicios generales sufridos por un individuo como resultado de una violación dolosa o intencionada de las disposiciones de las secciones 552a (g) (1) (C) o (D) del título 5 del Código de los Estados Unidos;

(iv) si y de qué modo debieren ser aplicadas las normas de seguridad y confidencialidad de los registros, prescritas por la sección 552a (e) (10) de dicho título, cuando un registro fuere revelado a una persona distinta de un órgano.

(C) La Comisión podrá estudiar aquellas otras actividades de información personal que fueren necesarias para ejecutar la política del Congreso recogida en la presente ley, si bien la Comisión no investigará los sistemas de información llevados por organizaciones religiosas.

(3) Al realizar tal estudio, la Comisión deberá

(A) determinar qué disposiciones legales, decretos presidenciales, disposiciones reglamentarias, directrices y decisiones judiciales rigen las actividades objeto de estudio, y la medida en que las mismas son compatibles con los derechos de privacidad, proceso judicial y otras garantías de la Constitución;

(B) determinar en qué medida los sistemas de información de la Administración y privados afectan a las relaciones entre la Federación y los Estados o al principio de separación de poderes;

(C) examinar las normas técnicas y criterios que rigen los programas, directrices y prácticas, relativos a la obtención, petición, tratamiento, uso, acceso, integración, difusión y transmisión de información personal; y

(D) en la máxima medida que fuere posible, reunir y utilizar conclusiones, informes, estudios, transcripciones de debates parlamentarios y recomendaciones de entes administrativos, legislativos y privados, instituciones, organizaciones e individuos, que hicieren referencia a los problemas objeto de estudio por parte de la Comisión.

(d) Sin perjuicio de sus otras funciones, compete a la Comisión:

(1) requerir la ayuda de los titulares de los Departamentos, órganos y organismos de la Administración federal y de las Administraciones estatales y locales, y otras personas, con miras al ejercicio de las funciones que le competen en virtud de la presente ley;

(2) previa petición al efecto, asistir a los órganos federales en el cumplimiento de lo prescrito en la sección 552a del título 5 del Código de los Estados Unidos;

(3) determinar si debería ser prohibida por ley la recogida por los órganos federales de determinadas clases de información, de entre aquellas cuya recogida violaría el derecho de privacidad del individuo; y

(4) previa petición al efecto, preparar una legislación uniforme para su uso por los Estados y las Administraciones locales en la concepción de procedimientos de manejo, llevanza y difusión de información personal al nivel estatal y local, y prestar a las Administraciones estatales y locales la asistencia técnica que tales Administraciones precisaren para la preparación y ejecución de dicha legislación.

(e) (1) Para el cumplimiento de las funciones que en virtud de

la presente sección le competen, la Comisión podrá realizar inspecciones, celebrar sesión y resolver en cualesquiera momentos y lugares, celebrar audiencias, recibir declaraciones, requerir mediante citación con cláusula penal la asistencia de testigos y la producción de libros, registros, papeles, correspondencia y documentos, recibir juramentos, ordenar la impresión y encuadernación de materiales, y efectuar gastos, según la Comisión considerare oportuno. Sólo se librarán citaciones con cláusula penal previo voto afirmativo de la mayoría de todos los miembros de la Comisión. Las citaciones con cláusula penal serán libradas con la firma del presidente o de cualquier miembro de la Comisión designado al efecto por el presidente y serán entregadas por cualquier persona designada al efecto por el presidente o por dicho miembro. Cualquier miembro de la Comisión podrá recibir juramentos o declaraciones solemnes a quienes comparecieren como testigos ante la Comisión.

(2) (A) Cada departamento, órgano y organismo de la rama ejecutiva estará facultado para facilitar a la Comisión, previa petición del presidente, la información, datos, informes, y cualquier otra ayuda que la Comisión estimare necesaria para el cumplimiento de las funciones que en virtud de la presente sección le competen. Siempre que el titular del departamento, órgano u organismo elevare un informe en virtud de lo dispuesto en la sección 552a (o) del título 5 del Código de los Estados Unidos, se remitirá a la Comisión copia de tal informe.

(B) Para el cumplimiento de las funciones y el ejercicio de las facultades que, respectivamente, competen a la Comisión en virtud de la presente sección, la Comisión podrá aceptar de cualquiera de tales departamentos, órganos u organismos, u otras personas, cualquier dato identificable con respecto a un individuo, si tal dato fuere necesario para el cumplimiento de tales funciones y facultades. En cualquier supuesto en que la Comisión aceptare tal información, deberá velar porque la información sea usada solamente para el fin para el cual hubiera sido facilitada, debiendo la información, una vez cumplido tal fin, ser destruida o devuelta al departamento, órgano, organismo u otra persona de quien hubiera sido obtenida, según procediere.

(3) La Comisión tendrá facultad para:

(A) nombrar a un director ejecutivo y el personal técnico adicional que fuere necesario, fijando asimismo sus respectivas retribuciones, sin ajustarse al efecto a las disposiciones del título 5 del Código de los Estados Unidos que rigen en materia de nombramientos de la función pública competitiva, ni a las del capítulo 51 y del subcapítulo III del capítulo 53 de dicho título que hacen referencia a la clasifi-

cación de puestos de trabajo y a los niveles retributivos de la General Schedule, sin que en ningún caso las retribuciones excedan del nivel máximo correspondiente al grado GS-18 de la General Schedule previsto en la sección 5332 de dicho título; y

(B) contratar servicios temporalmente y con carácter intermitente, en la misma medida en que lo autoriza la sección 3109 del título 5 del Código de los Estados Unidos.

La Comisión podrá delegar cualesquiera de sus funciones en el personal de la Comisión que la misma designare, pudiendo autorizar sucesivas redelegaciones de funciones según se estimare conveniente.

(4) La Comisión estará autorizada para:

(A) aprobar, modificar y abrogar disposiciones reglamentarias reguladoras de la forma de sus actividades, organización y personal;

(B) concluir contratos u otros convenios, o modificaciones de los mismos, con cualquier Administración, departamento, órgano u organismo de los Estados Unidos, o con cualquier persona, razón social, asociación o sociedad mercantil, pudiendo tales contratos, convenios, o modificaciones de los mismos, ser concluidos sin contraprestación legal, sin garantía de ejecución ni otras garantías, y sin ajustarse a lo dispuesto en la sección 3709 de las Leyes Revisadas, versión modificada (título 41 sección 5 del Código de los Estados Unidos, sección 5).

(C) efectuar los pagos anticipados, pagos de aumentos y otros pagos, que la Comisión estimare necesarios al amparo de la presente ley, sin ajustarse a las disposiciones de la sección 3648 de las Leyes Revisadas, versión modificada (título 31, sección 529, del Código de los Estados Unidos);

(C) llevar a cabo cuantos otros actos fueren necesarios para el cumplimiento de las funciones que en virtud de la presente sección le competen.

(f) (1) Cada uno de los miembros, o el miembro respectivamente, de la Comisión, que fuere directivo o empleado de los Estados Unidos prestará servicio en la misma sin percibir retribución adicional alguna, si bien continuará percibiendo la retribución que correspondiera a su puesto de trabajo ordinario cuando tuviere encomendado el cumplimiento de las tareas atribuidas a la Comisión.

(2) Los miembros de la Comisión a los cuales no fuere aplicable lo dispuesto en el parágrafo (1) percibirán dietas de una cuantía igual al nivel diario máximo correspondiente al grado GS-18 de la General Schedule cuando tuvieren encomendado el cumplimiento de las tareas atribuidas a la Comisión.

(3) Todos los miembros de la Comisión serán indemnizados de los gastos de desplazamiento, manutención y otros gastos necesarios que

les fueren irrogados como consecuencia del cumplimiento de las tareas atribuidas a la Comisión.

(g) Siempre que fuere procedente, y, en todo caso, por medio de una Memoria Anual, la Comisión informará al Presidente y al Congreso de las actividades realizadas en cumplimiento de las disposiciones de la presente sección. La Comisión elevará un informe final al Presidente y al Congreso acerca de las conclusiones obtenidas como resultado del estudio prescrito por la subsección (b) (1) de la presente sección, dentro del plazo máximo de dos años, a contar de la fecha en la cual hubieran quedado nombrados todos los miembros de la Comisión. La Comisión dejará de existir una vez transcurridos treinta días subsiguientes a la fecha en la cual su informe hubiera sido elevado al Presidente y al Congreso.

(h) (1) El miembro, directivo o empleado de la Comisión que, por razón de su empleo o puesto oficial, tuviere en su poder registros dependientes de órganos administrativos, que contuvieren información identificable con respecto a un individuo y cuya revelación estuviere prohibida por la presente sección, o tuviere acceso a tales registros, y, a sabiendas de que la revelación está prohibida, dolosamente revelare tal información de cualquier manera a cualquier persona u órgano que no tuviere derecho a recibirla, será culpable de delito leve y castigado con multa cuya cuantía no excederá de 5.000 dólares.

(2) La persona que, a sabiendas y dolosamente, solicitare u obtuviere de la Comisión, aduciendo falsos motivos, un registro concerniente a un individuo será culpable de delito leve y castigada con multa cuya cuantía no excederá de 5.000 dólares.

SECCION 6

Compete a la Oficina de Dirección y Presupuesto:

(1) formular directrices y dictar normas reglamentarias para su aplicación por los órganos en la ejecución de las disposiciones de la Sección 552a del título 5 del Código de los Estados Unidos, añadida por la sección 3 de la presente ley; y

(2) ejercer de manera continuada la asistencia y supervisión de la ejecución por los órganos de las disposiciones de dicha sección.

SECCION 7

(a) (1) Será ilegal para cualquier órgano de la Administración federal, estatal o local, denegar a un individuo un derecho, beneficio o privilegio concedido por disposición legal, en razón de la negativa de tal individuo a revelar su número de cuenta de la Seguridad Social.

(2) Lo dispuesto en el parágrafo (1) de la presente subsección no se aplicará.

(A) a la revelación impuesta por ley federal, o

(B) a la revelación de un número de la Seguridad Social a un órgano federal, estatal o local que llevare un sistema de registros existente y en funcionamiento con anterioridad al primero de enero de 1975, si tal revelación estuviere impuesta en virtud de ley o reglamento aprobado antes de dicha fecha a efectos de la comprobación de la identidad de un individuo.

(b) El órgano de la Administración federal, estatal o local que requiriere a un individuo a que revelare su número de cuenta de la Seguridad Social informará a dicho individuo acerca de si tal revelación es obligatoria o voluntaria, de la base legal o de otra índole en cuya virtud fuere solicitado el número, y del uso que de la misma hubiere de hacerse.

SECCION 8

Las disposiciones de la presente ley estarán en vigor en la fecha de promulgación y con posterioridad a la misma, salvo que las modificaciones aportadas por las secciones 3 y 4 entrarán en vigor una vez transcurridos 270 subsiguientes al día en que la presente ley hubiere sido promulgada.

SECCION 9

Se autoriza la habilitación de la suma de 1.500.000 dólares en los presupuestos de los años fiscales 1975, 1976 y 1977, para la ejecución de las disposiciones de la sección 5 de la presente ley, si bien no podrán ser gastados más de 750.000 dólares durante ninguno de dichos años fiscales.

Aprobada el 31 de diciembre de 1974.