

# El Proyecto de Ley de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal: la excepcionalidad como norma

Diego LOPEZ GARRIDO

Ha hecho falta que la policía descubra y haga pública la detención de personas que, supuestamente, traficaban con datos personales obtenidos de fuentes públicas, de forma fraudulenta, para lo que organizaciones no gubernamentales han venido predicando como voz que clama en el desierto tome cuerpo y haga visible la situación de *alegalidad* en cuanto a la gran cuestión de la protección de la intimidad frente al uso abusivo de la tecnología informática.

Los traficantes de datos personales inculpados parece que poseían los correspondientes a más de la mitad de la población española. Es espectacular; pero, en realidad, corresponde a la enorme potencia que la tecnología del tratamiento automatizado de datos permite. Una tecnología que va a velocidad de vértigo. Tanta que cuando vea la luz el Proyecto de Ley, hoy en el Parlamento, *sobre regulación del tratamiento automatizado de los datos de carácter personal*, seguramente estará ya sobrepasado por la realidad. Vivimos en una «sociedad de vigilancia intensiva», por emplear una terminología médica muy adecuada a nuestro tema.

Probablemente la causa de ello es que la información resulta ser casi en el siglo XXI un recurso esencial, celosamente guardado, para la gestión burocrática (pública y privada) de la política económica global. Aquí está la raíz de la multiplicación exponencial de la fuerza de trabajo destinada a las tecnologías del «control», y del desequilibrio entre quienes proveen información y quienes la guardan.

La naturaleza nueva del fenómeno de la telemática, y su amenaza para las libertades, reside en que aquí el observador nunca es visto. La posible violación de la intimidad no se revela a los individuos que sufren, anestesiados, esa violación. Se trata de una vigilancia que es nutrida por el propio sujeto/objeto de la información (*subject data*).

Para los españoles, desde hace algunos días está ya claro que el comercio sobre información personal es un suculento negocio. Pero esto no autoriza a sentenciar interesadamente, como hizo el Ministro para las Administraciones Públicas, que la amenaza proviene principalmente del sector privado. De hecho, la información que poseían las personas en su día detenidas se obtuvo, en todos los casos, de fuentes públicas, de diversos Ministerios. El Estado es quien maneja la mayor cantidad de información personal existente en éste y en otros países de nuestro entorno. La Administración Fiscal; la Administración Policial, con su modelo analítico de orien-

tación preventiva y con el flujo transnacional de datos consecuencia de los delitos transnacionales; la Administración Sanitaria, manejando dosieres médicos extremadamente sensibles, son tres gigantes ejemplos de la amenaza que supone para la intimidad personal el poder informativo del Estado, y la necesidad de su control seguro.

Naturalmente, la dimensión privada del problema es indudable. No sólo por las implicaciones comerciales de la tecnología de los «nichos del mercado», que requiere una visualización lo más afinada posible de los sectores o segmentos de población que pueden ser sensibles a un determinado producto. Hay muchos otros ejemplos. Así, el caso del reclutamiento laboral. Nadie sabe si las empresas especializadas en selección de personal guardan en sus ficheros automatizados datos sensibles que descartan de antemano a ciudadanos o ciudadanas cuyas actividades sindicales o políticas, cuya religión o cuyas ideas les hacen indeseables para obtener determinados trabajos. Esas personas nunca lo sabrán.

Los flujos transfronterizos de datos son la expresión más sofisticada de la potencia de la informática unida a la de las telecomunicaciones. La construcción europea no es ajena a ello y aquí ha adquirido sus tintes más siniestros. El Convenio conocido como Acuerdo Schengen, pensado para el control y la represión de la inmigración en determinados países europeos, tiene como uno de sus pilares el Sistema Informático Schengen, que interconectará a las policías de todos esos países por ejecutar como un solo hombre la decisión tomada por cualquiera de ellas prohibiendo la entrada, sancionando o denegando el asilo político a cualquiera de esos inmigrantes.

Hasta hoy no se puede decir que hubiese un clamor popular por esta laguna en el desarrollo constitucional (no olvidemos que el artículo 18.4 de la Constitución Española prevé expresamente una Ley que limite el uso de la informática en cuanto atente a la intimidad personal). A eso hay que añadir la hostilidad de Ministerios como el de Hacienda o Interior para explicarnos por qué ningún Gobierno ha sido capaz de llevar al Parlamento un Proyecto de Ley en desarrollo del artículo 18.4 de la Constitución hasta su publicación en el *Boletín Oficial de la Cortes Generales* de 24 de julio de 1991.

Y ello a pesar de la insistencia de algunos en denunciar ese vacío equivalente a la ley de la selva. La Asociación Pro Derechos Humanos envió hace casi un lustro a los grupos parlamentarios un borra-

dor de Proyecto de Ley, que luego fue asumido por el grupo de Izquierda Unida y presentado infructuosamente por dos veces en el Congreso de los Diputados.

España seguía incumpliendo el Convenio del Consejo de Europa, de 28 de enero de 1981, sobre protección de las personas en lo referente al tratamiento automatizado de datos personales. Ese Convenio fue ratificado por España en 1984 y nunca lo desarrolló. Cuando la Comisión Europea culminó una propuesta de Directiva relativa a la protección de las personas en lo referente al tratamiento de datos personales (*Diario Oficial de la Comunidad Europea* de 5 de noviembre de 1990), al Gobierno español no le quedó ya ninguna salida más que preparar, aunque fuera a regañadientes, el Proyecto de Ley que en estos días debate el Parlamento.

Ante estos antecedentes, y sensibilizados por los hechos a que hacemos alusión al principio de este artículo, se muestra con toda claridad la irresponsabilidad de unos Gobiernos que han mantenido en el vacío legal conductas tan reprobables como las que han sido objeto de represión policial y que van a ser difícilmente objeto de represión judicial.

## LA PROPUESTA DE DIRECTIVA DE LA COMUNIDAD EUROPEA

El Proyecto de Ley español se inspira fuertemente en la propuesta de Directiva elaborada por la Comisión Europea a que hacemos mención anteriormente. Por ello, creo que no estaría de más que dedicásemos algunos párrafos a esta propuesta de Directiva, que seguramente pronto será aprobada.

La Comunidad Europea no se ha caracterizado precisamente por su agresividad en la protección de los Derechos Humanos. Sus objetivos han sido descaradamente economicistas y, por tanto, la sensibilidad humanitaria quedaba fuera de los intereses comunitarios. La propuesta de Directiva en cuestión significa un leve acercamiento a esa sensibilidad pero, no nos engañemos, la razón de su elaboración, de su existencia, es básicamente comercial. Como dice la Comunicación de la Comisión Europea sobre *la protección de las personas en lo referente al tratamiento de datos personales en la Comunidad y la seguridad de los sistemas de información*, de 24 de septiembre de 1990, la diversidad de enfoques nacionales en cuanto a la protección de las personas en lo referente al tratamiento automatizado de datos personales, y la ausencia de un sistema de protección a escala comunitaria, constituyen un obstáculo a la realización del mercado interior. Si los derechos fundamentales de los interesados, en particular el derecho a la intimidad, dice la Comisión, no se garantizan a nivel comunitario, puede verse entorpecido el intercambio transfronterizo de datos, que se ha hecho indispensable para las actividades de las empresas y de los organismos de investigación, y para la colaboración entre las Administraciones de los Estados miembros, en el marco del espacio sin fronteras contemplado en el artículo 8A del Tratado CEE.

Por otra parte, ir a un «enfoque comunitario» en

materia de protección de las personas en lo referente al tratamiento de datos personales, constituye un requisito esencial para el desarrollo de la industria de la informática y de los servicios telemáticos de gran valor añadido. De ahí que la Comisión haya elaborado otra propuesta de Directiva relativa a la protección de los datos personales y de la intimidad en relación con las redes públicas digitales de telecomunicación, y en particular, la red digital de servicios integrados (RDSI) y las redes móviles digitales públicas (*Diario Oficial de la Comunidad Europea* de 5 de noviembre de 1990). Este aspecto de la telecomunicación y su impacto en la intimidad personal ha sido, por cierto, obviado por el Proyecto de Ley español, que nace así con una importante limitación de origen.

En fin, la penetración de la informática en todas las esferas de las actividades económicas y la aparición de sistemas de comunicación globales que facilitan la integración de diversas actividades, constituyen, a juicio de la Comisión Europea, un nuevo reto que hace necesaria una «protección» adaptada a los riesgos derivados de posibles fallos técnicos o humanos.

El objetivo de la Directiva comunitaria es facilitar la circulación de datos personales dentro del espacio comunitario. La Comunicación de la Comisión a que hacemos referencia es absolutamente sincera al confesar que lo que pretende es que, dado que todas las personas deben gozar en cada uno de los Estados miembros de una protección equivalente de «alto nivel» en lo referente al tratamiento de datos personales —ése es el objetivo a cubrir por la Directiva— los Estados miembros no podrán en el futuro imponer restricciones a la circulación de dichos datos dentro de la Comunidad invocando la protección del interesado.

En resumen, la Directiva comunitaria no se sitúa, y ése es uno de los errores de fondo del mimético Proyecto de Ley del Gobierno socialista, dentro del nivel de máxima protección de la intimidad, porque su finalidad es otra. Trata de establecer unos mínimos de seguridad para los datos personales que permitan disolver cualquier obstáculo para la circulación acelerada de información personal, para el progreso del sector informático y de las telecomunicaciones, para, en definitiva, también en este sector económico permitir llegar hasta sus últimas consecuencias en la idea del Mercado Interior Único. No se trata de criticar a la Comunidad Europea porque ésa sea la finalidad de la Directiva, ya que se mueve estrictamente en los objetivos lícitos de la Comunidad. Lo que es criticable es que un Proyecto de Ley adopte una protección de *mínimos*, como la que establece la Directiva, para legitimarse, cuando el mandato constitucional de protección de la intimidad y la filosofía de protección de un derecho fundamental como ése exigirían mucha mayor audacia respecto de las amenazas provenientes, no sólo del sector privados sino, fundamentalmente, de los organismos públicos, que son los que controlan y manejan el mayor número de datos personales incluidos en ficheros automáticos.

## EL PROYECTO DE LEY ESPAÑOL

El contenido del Proyecto de Ley podría resumirse diciendo que hace una correcta regulación de los principios básicos de protección de la intimidad respecto del tratamiento de datos personales por entidades públicas y privadas en ficheros automatizados y que, al establecer las excepciones a tales principios, echa por tierra la anterior labor.

Los principios básicos están en los artículos 4, 5, 6, 7 y 11. No hay mucho que objetar a esa regulación, como decíamos. Dada las características de este breve comentario no creo que proceda extenderse en hacer una glosa o resumen del contenido de tales preceptos. Las prescripciones establecidas en el Convenio del Consejo de Europa de 1984 son básicamente adoptadas.

Asimismo, los derechos de las personas de acceso, rectificación, bloqueo (concepto extraído de la Ley alemana) y cancelación, están recogidos. No se trata de una regulación modélica, pero tampoco pueden hacerse críticas profundas. Quizá la más importante sería la de la generosidad con la que se remite la regulación concreta de todos estos importantes aspectos al Reglamento. En cuanto a los ficheros de titularidad privada, su regulación es en términos generales, adecuada en el Proyecto de Ley.

Hasta aquí la norma o, mejor dicho, la aparente norma, ya que, cuando nos vamos a los artículos relativos a los ficheros de titularidad pública podemos apreciar con toda claridad que la excepción es la que se convierte en norma. Los artículos 19, 20, 21 y 22 son, desde el punto de vista de la protección de la intimidad personal, muy negativos. Vamos a examinarlos brevemente.

El artículo 19 del Proyecto dice:

«1. Los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones *no serán cedidos* a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, *salvo cuando la cesión hubiese sido prevista por las disposiciones de creación del fichero o por disposición posterior de igual o superior rango que regule su uso.*»

2. Podrán, en todo caso, ser objeto de cesión los datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra.»

Resulta extremadamente flexible esa posibilidad que la Ley establece de ceder datos de carácter personal cuando así hubiera sido previsto en una disposición de creación del fichero o en una disposición posterior de igual o superior rango que regule su uso. Esa disposición no tiene que ser una ley. Puede ser una norma de rango muy inferior, lo que va a dar lugar a las mayores arbitrariedades respecto de una cesión de datos que constituye, seguramente, el mayor de los peligros detectados en esta materia.

El artículo 20 se refiere a los ficheros automatizados creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal. Los apartados 2 y 3 del dicho artículo 20 dicen:

«2. La recogida y tratamiento automatizados para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad *sin consentimiento* de las personas afectadas, están limitados a aquellos supuestos y categorías de datos que *resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales*, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías, en función de su grado de fiabilidad.

«3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos a que hacen referencia los apartados 2 y 3 *del artículo siete*, podrán realizarse *exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta.*»

El artículo 20 está, sin duda, repleto de peligrosísimos conceptos jurídicos indeterminados. Las Fuerzas y Cuerpos de Seguridad van a poder recoger y tratar automatizadamente datos de carácter personal *sin consentimiento* de las personas afectadas cuando «resulte necesario para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales».

Más grave aún es lo relativo a lo que se ha llamado *datos sensibles*. Estos van a poder ser recogidos y tratados por las Fuerzas y Cuerpos de Seguridad también *sin consentimiento* de los afectados en los supuestos en que sea «absolutamente necesario para los fines de una investigación concreta».

Convendría hacer en este punto una referencia a la forma en que están definidos los datos personales sensibles en el Proyecto de Ley. A ellos se refiere el artículo 7, que dice lo siguiente en sus apartados 2 y 3:

«2. Sólo con consentimiento expreso del afectado podrán ser objeto de tratamiento automatizado los datos de carácter personal que revelen su ideología, religión o creencias.

3. Los datos de carácter personal que hagan referencia al *origen racial, a la salud y a la vida sexual* sólo podrán ser recabados, tratados automáticamente y cedidos cuando, *por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente.*»

El Proyecto de Ley entiende, pues, que, aún sin consentimiento del afectado, si lo dispone una ley, pueden almacenarse, tratarse automáticamente y cederse datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual. Resulta extremadamente incomprensible el que se necesite tratar automáticamente, almacenar o ceder datos que afectan a la intimidad más profunda de la personal. Quizá podría excluirse de lo anterior lo relativo a la salud, por las consecuencias de interés general que pudieran derivarse del no control adecuado de determinadas enfermedades. Sin embargo, el origen racial o las costumbres sexuales deberían estar erradicadas de cualquier tipo de fichero automatizado obtenido sin el consentimiento del

afectado. Seguramente en el fondo de esta cuestión está la preocupación por la inmigración y las exigencias represivas que se derivan de la firma del Acuerdo Schengen. En cuanto a la vida sexual se nos acaba la imaginación para pensar cuál puede ser el interés en que datos tan íntimos puedan ser legalmente recabados y tratados en ficheros automatizados.

Pues bien, estos datos llamados sensibles, es decir, aquellos que afectan a la intimidad más estricta de la persona, a su dignidad como tal, al ámbito más profundo de su soberanía interior, pueden ser recogidos y almacenados en ficheros automatizados por las Fuerzas y Cuerpos de Seguridad en las abstractas circunstancias a que se refiere el artículo 20 del Proyecto de Ley.

Lo más grave de esa regulación aparece en el siguiente artículo, en el 21, del cual se deduce la imposibilidad de control sobre el uso o abuso que de esa potestad vayan a hacer las Fuerzas y Cuerpos de Seguridad. En efecto, el artículo 21 del Proyecto dice lo siguiente:

«1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior, *podrán denegar el acceso, la rectificación o la cancelación* en función de los peligros que pudieran derivarse para la *defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros, o las necesidades de las investigaciones* que se estén realizando.

2. Los responsables de los ficheros de la *Hacienda Pública* podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del Organismo competente de cada Comunidad Autónoma en el caso de ficheros automatizados mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones Tributarias Autonómicas, quien deberá asegurarse de la procedencia o improcedencia de la denegación.»

Como se deduce del apartado 1 del artículo 21, no va a ser posible controlar el uso de la potestad concedida por el artículo 20 a las Fuerzas y Cuerpos de Seguridad porque éstas podrán denegar el acceso, la rectificación o la cancelación de los datos sensibles a las personas afectadas en función de «los peligros que pudieran derivarse para la defensa del Estado a la Seguridad Pública, la protección de los derechos y libertades de terceros, o las necesidades de las investigaciones que se estén realizando». Es decir, los peligros que pudieran derivarse de prácticamente todo tipo de eventualidad. Así que, la potestad del artículo 20 de las Fuerzas y

Cuerpos de Seguridad en relación con los datos sensibles queda fuera de control. Ni siquiera del control del Director de la Agencia de Protección de Datos, que es el Organismo pensado para ello en el Proyecto de Ley, ya que lo único que le permite el artículo 21 en su apartado 3 es que pueda «asegurarse de la procedencia o improcedencia de la denegación». Una frase verdaderamente inescrutable, y rigurosamente inútil.

Las mismas consideraciones cabría hacer, matizadas por una materia tan diferente, respecto de los ficheros de la Hacienda Pública.

Las excepciones no acaban aquí. El artículo 22 consagra esa definición con que nos atrevemos a definir el Proyecto de Ley como algo que convierte lo excepcional en normal. Porque ese artículo limita extraordinariamente el derecho que el afectado tiene de ser informado de la finalidad de la recogida de datos de carácter personal, del carácter obligatorio o facultativo de su respuesta a las preguntas que le sean planteadas, de la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación, etc., previsto en el artículo 5 del Proyecto.

Asimismo se limita gravemente el derecho previsto en el artículo 15 del Proyecto de Ley de exigir la rectificación, cancelación o bloqueo de los datos que resulten inexactos. Lo mejor será que reproduzcamos a continuación la redacción del artículo 22 para corroborar esta apreciación:

«1. Lo dispuesto en los apartados 1 y 2 del artículo cinco no será aplicable a la recogida de datos cuando la información al afectado *impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas* o cuando afecte a la Defensa Nacional, a la Seguridad pública o la persecución de infracciones penales o administrativas.

2. Lo dispuesto en el artículo catorce y en el apartado 1 del artículo quince no será de aplicación si, *ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección*. Si el órgano administrativo responsable del fichero automatizado invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.»

Ante esta serie de excepciones que devalúan de una forma muy notable los principios generales establecidos en los primeros artículos del Proyecto de Ley, resulta incluso de importancia menor el que el Director de la Agencia de Protección de Datos tenga un origen gubernamental.

El Director de la Agencia de Protección de Datos, órgano tutelador de la legislación de protección de datos, es nombrado por el Gobierno por cuatro años y tiene un determinado estatuto de independencia, al que se refiere el artículo 25 del Proyecto de Ley,

