LOS RIESGOS DEL IDENTIFICADOR UNIVERSAL Y EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA

Jordi BARRATI ESTEVE

SUMARIO: I. *Resumen.* II. *Introducción.* III. *El número de identificación personal (NIP).* IV. *El caso español. V. La dignidad humana y el libre desarrollo de la personalidad.* VI. *Los principios de protección de los datos personales. La STC 143/1994.* VII. *Bibliografía.*

I. RESUMEN

La comunicación aborda la regulación de los números de identificación personal. Se trata de un aspecto del derecho a la autodeterminación informativa, es decir, del conjunto de facultades que se otorgan a los individuos para que puedan controlar de forma efectiva el flujo de datos personales que se encuentran en poder de otras instancias.

Tal derecho se ha consolidado en las últimas décadas a raíz del crecimiento de las aplicaciones informáticas ya que su enorme potencial ha suscitado fundados recelos sobre el uso de los datos que proporcionamos tanto a la administración pública como a los actores privados. El peligro consiste en la aparición de ficheros que, incluyendo datos entregados en operaciones aisladas, permitan la obtención de un retrato completo de cada una de las personas.

Los códigos numéricos individuales agravan esta situación ya que facilitan la fusión de distintos ficheros. Al vincular cada persona con una clave inmutable, resultará extraordinariamente sencillo encontrar todos los datos relacionados con ella que obren en un conjunto aparentemente disperso de archivos informáticos.

Varios países han diseñado mecanismos específicamente destinados a evitar estos usos perversos de los códigos numéricos. Destaca, por ejemplo, el caso de Portugal ya que el artículo 35 de su texto constitu-

cional prohibe la existencia de un identificador numérico nacional para cada individuo.

El trabajo expone los peligros de un uso incontrolado de la clave numérica individual, describe la situación existente en España, donde el ordenamiento jurídico no contempla garantías concretas, y analiza posteriormente distintas posibilidades de reducir su impacto negativo.

II. Introducción

Es sabido que la protección de los datos personales constituye uno de los elementos fundamentales de cualquier ordenamiento que se proponga, como señala el artículo 18.4 de la Constitución española, limitar el uso de la informática con el fin de proteger los derechos y libertades de los ciudadanos. La consolidación normativa y doctrinal del denominado derecho a la autodeterminación informativa ha propiciado la aparición de un amplio abanico de facultades e instituciones que permiten al ciudadano controlar los usos que otras personas hacen de sus datos.[1]

1 La Ley Orgánica 5/1992 de Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD) se encargó de desarrollar las previsiones del artículo 18.4 de la Constitución española. Posteriormente, la Directiva comunitaria 95/46 motivó la aprobación de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal-LOPD (*cfr*. la resolución de los recursos de inconstitucionalidad interpuestos contra esta norma en SSTC 290 y 292/2000). Destaca asimismo la Ley 8/2001 de Protección de Datos de Carácter Personal en la Comunidad de Madrid, único caso en el que se ha creado una autoridad autonómica de control para realizar, en los ámbitos que permite la LOPD, las funciones que, a nivel general, realiza la Agencia de Protección de Datos. Consúltese, por último, el Convenio 108 del Consejo de Europa y la Carta de los Derechos Fundamentales de la Unión Europea (artículo 8o.).
Por otra parte, el Tribunal Constitucional federal alemán aprovechó un recurso presentado contra la ley del censo para consolidar jurisprudencialmente, en decisión de 15 de diciembre de 1983 (BVerfG, 65.1), el derecho a la autodeterminación informativa. La inicial configuración de la protección de los datos personales como una garantía instrumental del derecho a la intimidad evidenció ciertas insuficiencias ya que los datos a proteger no podían reducirse a aquéllos que conforman tradicionalmente el núcleo íntimo de las personas. Tampoco era satisfactoria la tutela fundamentalmente represiva que caracteriza al derecho a la intimidad ya que, sin descuidar la sanción, se exigía la articulación de medidas preventivas. Todo ello generó la aparición de un nuevo derecho.
Pese a que la sistemática de la Constitución de 1978 y el tenor literal del apartado cuarto del artículo 18 inducen a mantener la mencionada relación entre la intimidad y la protección de datos, la corriente doctrinal mayoritaria en España (*cfr*. Lucas Murillo de la Cueva, 1990) ha seguido la estela alemana al reconocer la existencia de un nuevo derecho. La STC 294/1993 asumió esta tendencia y las dos decisiones anteriormente

Su cesión, es decir, su transmisión a una tercera instancia, se erige como uno de los principales peligros ya que resulta complicado que el ciudadano pueda controlar de modo efectivo sus datos personales si la persona o institución a la que se los ha proporcionado puede comunicarlos libremente a otros interesados.

Tal peligro se experimenta de modo relevante, aunque no exclusivo, en la actuación de los poderes públicos ya que, con el progreso acelerado de las tecnologías de la información y en un escenario donde todas las administraciones apuestan por su informatización interna y externa, no es descabellado pensar en un mecanismo que permitiera conocer todos los datos que, relacionados con un individuo, obran en los expedientes de una determinada Administración.[2] Será fácil, por lo tanto, agrupar esas facetas de la "personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado" (exposición de motivos de la LORTAD).[3]

citadas lo han confirmado (*cfr*. el voto particular del magistrado Manuel Jiménez de Parga en STC 290/2000).
El objetivo primordial del derecho a la autodeterminación informativa consiste en otorgar al ciudadano un haz de facultades que le permita decidir los datos personales que pueden ser conocidos por otras personas y el uso que va a hacerse de ellos. La creación de organismos independientes específicamente dedicados a estos fines, la obligación de inscribir en un registro público todos los ficheros que contengan datos personales o la necesidad de recabar el consentimiento del titular de los datos constituyen algunos de los pilares fundamentales de este derecho. Se reconoce asimismo la necesidad de proporcionar una amplia información sobre, entre otras cosas, las características del fichero, su ubicación, sus responsables o su finalidad. El afectado dispone, por último, de los derechos de acceso al fichero, rectificación de los datos erróneos y cancelación.

2 La Comunidad de Madrid ya ofrece, de hecho, esta información. La Agencia de Protección de Datos de dicha Comunidad —APDCM— creó la denominada *Sección de interesados* donde los ciudadanos pueden inscribirse con el fin de obtener información sobre los ficheros en que se contengan datos personales de su titularidad. A estos efectos los responsables de fichero comunicarán, cada tres meses, a la Sección de Interesados las variaciones experimentadas en los ficheros en cuanto a los afectados inscritos (artículo 17 del Estatuto de la Agencia, Decreto 22/1998 de 12 de febrero; *cfr*. APDCM, 2001: 2 59-60). Se trata lógicamente de un instrumento destinado a perfeccionar el derecho a la autodeterminación informativa, pero también refleja la notable sencillez con la que se pueden unir datos que hemos ido proporcionando de forma separada.

3 El debate sobre el *anonimato*, es decir, la capacidad de actuar sin verse obligado

III. El número de identificación personal (NIP)

La concentración de datos está al alcance de las modernas tecnologías informáticas, pero hay ciertos elementos que pueden facilitar dicha operación. La existencia de un código numérico individual es uno de ellos ya que, al otorgar a cada persona un identificador único y exclusivo, la operación de cruzar los diferentes ficheros en busca de todos los datos vinculados a dicha clave se convierte en algo sumamente sencillo.[4] Se aumenta la capacidad de procesamiento, pero también se afecta a la configuración del derecho a la autodeterminación informativa ya que disminuyen las facultades de control del ciudadano sobre sus propios datos. José Antonio Martín Pallín, magistrado del Tribunal Supremo, alude a este peligro con tonos especialmente dramáticos al señalar que "detrás de la utilización de los números como signos de identidad existe un espíritu totalitario... cualquier persona sensible y con espíritu democrático debe rechazar de inmediato este primer impulso y meditar seriamente sobre las consecuencias negativas y antidemocráticas que acarrea la implantación del sistema" (1997, p. 62).[5]

a desvelar la identidad, constituye uno de los grandes retos de la actual transformación tecnológica y social (*cfr*. Marx, 2001 y Wallace, 1999). Es usual referirse a Internet como un territorio donde tal fenómeno alcanza sus cotas más elevadas, pero hay que ser conscientes de que, desde hace décadas, se está librando una lucha silenciosa entre los partidarios de una arquitectura informática que respete y fomente la libertad y los defensores de un control público de los mecanismos más sensibles de la red. Es significativo, en este sentido, que se considere "que a la nostra època la difusió o el control de la tecnologia de xifratge s'ha convertit en un criteri definidor per a saber en quina mesura els governs confien en els seus ciutadans i respecten els seus drets" (Castells, 2001; 2001a, pp. 208-211). Las técnicas de cifrado permiten, en efecto, ocultar ciertos datos, mantienen el anonimato y dificultan, en consecuencia, la elaboración del mencionado retrato completo de la personalidad de un individuo. Los recelos de las autoridades estadounidenses al uso privado de estos procedimientos reflejan nítidamente su trascendencia.

4 El reduccionismo numérico no es el único que puede utilizarse ya que se han probado, por ejemplo, códigos identificadores basados en huellas digitales o genéticas, Martín Pallín, 1997, p. 61.

5 Tras esta tensión subyace, como en otros casos, la lucha entre la eficacia administrativa y la protección de un derecho fundamental. El código universal acelera la gestión administrativa, pero también conlleva serias repercusiones para la dignidad de la persona y su libre desarrollo. Se hace preciso, en consecuencia, buscar un equilibrio entre ambos factores (*cfr*. Valero Torrrijos, 2001, pp. 260 y 261). La Constitución favorece esta operación al ofrecer tanto un amplio abanico de garantías para los derechos

Diversos países han presenciado un prolongado debate sobre la conveniencia de introducir un número o un documento nacional de identidad.[6] No es éste el lugar para ofrecer un exhaustivo estudio comparado,[7] pero debemos aludir, como mínimo, al artículo 8.7 de la ya citada Directiva comunitaria 95/46 en el que se asigna a los estados miembros la misión de determinar "las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento". A nivel estatal, sobresale la Constitución portuguesa de 1976 ya que, además de ser el primer texto constitucional que recogió la tutela de los datos personales, incluye expresamente la prohibición del mencionado código. El quinto apartado de su artículo 35 reza como sigue: "É proibida a atribuiço de um número nacional único aos cidados".[8]

Por otra parte, tanto en Francia como en Alemania, la elaboración de las primeras leyes sobre protección de datos estuvo condicionada por el

y libertades como una referencia a los principios de actuación de la Administración Pública entre los que se incluye la eficacia (artículo 103.1, CE). Debe destacarse asimismo que algunos autores relativizan la pretendida virtualidad de los sistemas universales de identificación. Davies llega a esta conclusión tras repasar sus consecuencias en la lucha contra el fraude fiscal, la inmigración ilegal y, de modo más genérico, en el cumplimiento de las leyes (1996, 6-8). Otros escritos alertan sobre el hecho de que "lo que inicialmente se plantea como un sistema de perfeccionamiento de la organización y métodos de producción se convierte en un instrumento de control que proporciona parcelas de poder hasta ahora nunca alcanzadas" (Martín Pallín, 1997: II).

6 Ambos elementos pueden establecerse de forma separada. Suele citarse el caso sueco donde, si bien se acepta un número individual, no existe un documento de identidad (Davies, 1996: 1).

7 Existe un abundante bibliografía sobre el tema. Pueden consultarse con sumo provecho las páginas que diversas organizaciones dedican a este asunto (Privacy International, 2001; Epic, 2001). Destaca asimismo la labor desarrollada por el Consejo de Europa ya que un estudio del Comité de Expertos en Protección de Datos describe la situación de cada país y ofrece un análisis general sobre las repercusiones de un identificador numérico universal (Consejo de Europa, 1991). Otros casos significativos como Australia o Nueva Zelanda en Davies, 1996.

8 Portugal ha desarrollado estas previsiones articulando un conjunto de garantías que impiden la aparición de un NIP multifuncional. Implantó, por ejemplo, un identificador fiscal, pero, si bien los primeros impresos tributarios reservaban una casilla para el número de identidad, la reforma de 1991 suprimió esa casilla con lo que, aun existiendo el identificador fiscal, las probabilidades de cruce de datos disminuían sensiblemente. Debe saberse asimismo que, en contraste con lo que sucede tanto en España como en otros países, el código fiscal no guarda similitud con el número de identidad. *Cfr*. Martín Pallín, 1997: IV.A.

debate sobre las consecuencias de un NIP multifuncional.[9] Destaca, en concreto, la ya mencionada decisión del Tribunal Constitucional federal alemán ya que, al analizar el identificador numérico, subrayó su trascendencia calificándolo como *paso decisivo* para registrar y catalogar completamente la personalidad de cada individuo (BVerfG, 65, 1, 57).

El Reino Unido y Estados Unidos también cuentan con una prolongada trayectoria de resistencia cívica a la implantación de mecanismos identificadores. El primero de ellos creó, durante la II Guerra Mundial, una tarjeta de identidad. Acabada la contienda, siguió utilizándose hasta que, en 1952, los tribunales declararon su invalidez dado que se empleaba para finalidades muy alejadas de los motivos de seguridad nacional esgrimidos al inicio (*cfr*. Gabb, 1999, pp. 31 y 32). Posteriormente, diferentes gobiernos han intentado, sin éxito, su reimplantación siendo una de las iniciativas más recientes el informe elaborado por el gabinete Major en 1995 (Home Office, 1995). La oposición suscitada obligó a retirarlo poco tiempo después, pero el atentado del 11 de septiembre de 2001 ha vuelto a poner sobre el tapete estas cuestiones ya que, al hilo de la reforma de las leyes antiterroristas, la existencia de mecanismos de identificación universales aparece como una técnica enormemente útil (*cfr*. Privacy International, 2001).

Lo mismo sucede en Estados Unidos donde, en los últimos meses (Clement, 2001), se ha recrudecido un debate ya existente en el que participan de modo especialmente intenso grupos "ultraliberales" *libertarians* (por ejemplo, Wolfe, 1998) y religiosos.[10] Debe destacarse la relevancia del número de inscripción en la seguridad social ya que, desde

9 En el primer caso, el Instituto Francés de Estadística intentó instaurar un número personal de identificación para todas las relaciones de los ciudadanos con las oficinas administrativas. El proyecto recibía la denominación, verdaderamente imprudente, de SAFARI —*Système automatisé pour les fichiers administratifs et le répertoire des individus*—, y suscitó una amplia oposición que desembocó tanto en la retirada del plan como en la redacción de una normativa tuteladora de los datos personales. Hoy en día, la *Commission Nationale de l'Informatique et des Libertés* se encarga de proteger a los ciudadanos frente a los abusos informáticos. En relación a los identificadores numéricos, todas sus finalidades deben estar expresamente autorizadas por un Decreto de Consejo de Estado, previo informe de la Comisión antes mencionada (artículo 18 de la Ley 78-17 relativa a la informática, a los ficheros y a las libertades).

10 Cabe mencionar, en este sentido, la existencia de varios litigios en los que, acudiendo a la objeción de conciencia, se han alegado motivos religiosos para rechazar la atribución de un código numérico a cada individuo (*cfr*. McDonald, 1999: II.3).

su creación en 1935, ha ido progresivamente ampliando su radio de acción hasta convertirse en el "de facto national identifier, despite constant rulings and legislation to the contrary" (Davies, 1996: 14; *cfr*. asimismo Hibbert, 2001).

Su considerable extensión y deficiente regulación (Garfinkel, 1995, p. 146; Twight, 2001, pp. 5-10) no conlleva, en todo caso, que debamos concebirlo como un numerador obligatoriamente presente en cualquier trámite. Aunque puede discutirse su verdadera eficacia, uno de los factores decisivos consiste en que cada fichero *público federal* requiere, desde 1975, autorización expresa para la utilización, con una finalidad determinada, del número de la Seguridad Social. En caso contrario, "it shall be unlawful... to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number" (7, *Privacy Act* de 1974; Us, Gao, 1999, pp. 2 y 7-12).

IV. El caso español

La creación en España de una clave única de identificación debe relacionarse con la aparición, en 1944, del Documento Nacional de Identidad (DNI). La normativa actualmente vigente admite explícitamente que su finalidad consiste en "generalizar su número como identificador unificado de gestión" (Preámbulo del Decreto 196/1976). Se señala posteriormente que "dicho número identificador ... figurará obligatoriamente en toda clase de documentos en los que... hubieren de constar los datos personales del titular" (artículo 4.3) y, por si quedara alguna duda, el siguiente apartado recuerda que, "con objeto de facilitar y agilizar la gestión administrativa, el número del documento nacional de identidad se adoptará como identificador numérico personal de carácter *general*" (artículo 4.4). Su gestión deberá respetar, en todo caso, el derecho a la intimidad (artículo 9.3 de la Ley 1/1992 de Protección de la Seguridad Ciudadana).[11]

11 Existen otros elementos que refuerzan la impresión de que el legislador español ha querido otorgar al documento nacional de identidad un uso muy amplio. De esta forma, el preámbulo del Decreto 1245/1985, por el que se reforman determinados aspectos del Decreto ya citado de 1976, anuncia la adición de "las normas necesarias para garantizar su eficacia probatoria en toda clase de procedimientos administrativos, propiciando su utilización en las relaciones privadas". *Cfr*. también su Disposición Adicional

Pese a esta regulación ampliamente favorecedora, no ha habido un debate público sobre los eventuales perjuicios de un uso generalizado del código individual.[12] La única ocasión en la que se suscitó cierta polémica obedeció a la aprobación del número de identificación fiscal (NIF). En contraste con lo que sucede en otros países, no se creó un identificador fiscal autónomo, sino que se importó la combinación del documento nacional de identidad (artículo 2o., b) del RD. 338/1990; Souvirón Morenilla, 1994: 186] que, como ya hemos visto, prevé su utilización generalizada en cualquier trámite. Todo ello, unido a la progresiva informatización de la Administración, implica que, "si no se sale al paso de esta tendencia, en corto plazo habremos implantado el número de identificación universal" (Martín Pallín, 1997, p. 68). Este autor recuerda que este peligro ha aumentado en los últimos años toda vez que han ido uniformándose los códigos particulares que utilizaban las diferentes secciones administrativas. La finalidad del número del DNI ya no se reduce a la identificación, sino que constituye, en multitud de ficheros, el código básico para localizar los datos relativos a una persona.

El debate doctrinal sobre la admisibilidad de un NIP universal ha utilizado dos líneas de reflexión. La primera de ellas, ante la ausencia de regulación específica, recurre a las cláusulas constitucionales donde se proclama la protección de la dignidad de la persona. La segunda aprovecha la regulación sobre la protección de datos para limitar el uso de un identificador universal.

V. La dignidad humana y el libre desarrollo de la personalidad

Cabe acudir, en primer lugar, al artículo 10.1 de la Constitución española. El Constituyente quiso ubicar, antes del listado detallado de cada uno de los derechos y libertades, un precepto donde se proclamaran los

Segunda.

12 Como señala Souvirón Morenilla, nos encontramos "ante problemas jurídicos de primera magnitud que me temo no ha resuelto nuestro ordenamiento en la debida forma, ni substantiva ni formalmente y que... no parecen preocupar ni merecer la atención de los ciudadanos (quizá porque nuestra sociedad hoy por hoy no ha logrado aún interiorizar ni articular en términos jurídicos operativos para la convivencia —como ciudadanía— ese supuesto, sólo supuesto, individualismo que nos caracteriza)" (1994, 184).

principios en los que se asienta el sistema constitucional. Se destaca que, entre otros elementos, "la dignidad de la persona (y)... el libre desarrollo de la personalidad... son fundamento del orden político y de la paz social".

Podrían existir, en este sentido, algunos métodos de comunicación de datos que, sin estar expresamente prohibidos, cabría considerar como inconstitucionales en virtud de la aplicación del artículo mencionado. Martín Pallín explora esta posibilidad y afirma que "la generalización del uso del número identificador que proporciona el documento de identidad puede afectar a la dignidad de la persona en cuanto que el ciudadano es tratado como una cifra abstracta con olvido de sus señas de identidad que más acusadamente caracterizan su personalidad y sus referencias en sociedad" (1997, p. 85).

La vinculación de todo individuo a una clave multifuncional implicaría desconocer que la dignidad "supone el reconocimiento de un status especial de la persona, que se sitúa por encima de los demás seres en virtud de su racionalidad" (Alegre Martínez, 1996, p. 17). Un NIP de esas características constituiría una deshumanización de la persona, degradaría su naturaleza y merecería, en definitiva, su prohibición.

Adviértase, por otra parte, que la propia LOPD, pese a no incluir ninguna referencia al problema señalado, parece compartir el razonamiento de fondo al eliminar la posibilidad de que un ciudadano sea valorado exclusivamente a través del prisma informático. Su artículo 13 señala, en este sentido, que:

> 1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.
>
> 2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad (*cfr*., asimismo, el artículo 15 de la Directiva 95/46 y Vizcaíno Calderón, 2001, pp. 183-188).

Nos encontraríamos ante otro supuesto en el que la espectacular extensión de los métodos informáticos puede conllevar la desnaturalización del procedimiento decisorio. Su aceptación implicaría una nueva derrota

del humanismo frente al apogeo tecnocrático que, en casos como los analizados, parece olvidar su originaria naturaleza instrumental y complementaria.[13] El debate, en definitiva, no puede estar centrado en la técnica, sino en el respeto a la dignidad humana y es por ello que ambos mecanismos, el NIP multifuncional y las valoraciones personales exclusivamente informáticas, serían inadmisibles.

Comparto esta posición, pero, a mi entender, es preferible recurrir a las garantías que, vinculadas a la protección de datos, se encuentran plasmadas, de forma expresa, en el ordenamiento. Estimo que, pese a no incluir una deseable referencia específica al problema aquí abordado, contienen los mecanismos suficientes para anular las consecuencias negativas de un código identificador único. Se evita asimismo que la dignidad se use "como comodín cada vez que nos encontremos en un atolladero" (Marina, 2000, p. 12).

VI. Los principios de protección de los datos personales. La STC 143/1994

Se parte de la base de que el NIP no es un factor meramente técnico y neutral, sino que constituye un auténtico dato personal y se halla sujeto a la normativa que regula dichos elementos.[14] Esta afirmación conlleva

13 Como advierte Gay Fuentes, este precepto "no está encaminado a garantizar el derecho a la intimidad sino a preservar un uso no abusivo de la informática, que implique una automaticidad excesiva de las decisiones privadas o administrativas" (1995, p. 85).

14 El artículo 2o., a) de la Directiva no deja lugar a dudas ya que, tras definir datos personales como "toda información sobre una persona física identificada o identificable", considera identificable a "toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un *número de identificación*". Además, el ya citado artículo 8.7 incluye el número nacional de identificación dentro de una categoría "especial" de datos que merecen un tratamiento específico. En España, tras admitir que los datos personales pueden ser de carácter numérico, el reglamento de desarrollo de la LOPD define identificación del afectado como "cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada" (artículo 1o.). No se menciona específicamente al NIP, pero no cabe duda que puede considerarse incluido en dicha definición (*cfr*. Aparicio Salom, 2000, p. 43).
Incluso en aquellos supuestos, como el Convenio 108 del Consejo de Europa, en los que resulta más difícil encontrar referencias explícitas a los números, cabe aplicar a los NIPs los principios de protección de datos ya que, como señala el informe del propio Consejo, "this view is premised on the fact that PINs are intimately linked to personal data processing... Even a serial number of no particular significance may open up a personal

serias consecuencias en aquellos países en los que el NIP refleja, en sí mismo, algún dato específicamente personal como la fecha de nacimiento, el estado civil, el sexo o el origen geográfico. En estos casos, los derechos de acceso y rectificación cobran gran virtualidad ya que pueden ejercitarse también sobre el código numérico para que, como mínimo, refleje con exactitud la realidad.

Otro principio —el de adecuación— señala que la creación de cualquier fichero debe poder justificarse en función de las actividades ejercidas por su responsable. Todos los datos deberán ser "adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido" (artículo 4.1, LOPD).[15] Se trata de un principio especialmente relevante a nuestros efectos ya que un NIP universal y multifuncional solo podrá ser admitido si podemos justificar adecuadamente la finalidad para la que ha sido creado.

Suele señalarse, en este sentido, que facilita el intercambio de información entre ficheros. También se destacan las dificultades que entrañaría la creación, en cada archivo, de un sistema autónomo de identificación (Us-Gao, 1999, pp. 12-13). Ambas ventajas deben contrastarse, sin embargo, con los peligros que encierra su existencia ya que los "PINs are the key to data processing" (Consejo de Europa, 1991, Concl. *i.*).[16] Sus evidentes ventajas pueden incluir poderosos efectos perversos y alentar un uso inapropiado de las modernas tecnologías. Es significativo, en este sentido, que diversos países mantengan un adecuado funcionamiento

data file containing sensitive information" (Consejo de Europa, 1991: 3).

15 Cabe plantearse, en este sentido, la corrección de la propia composición interna del NIP. Existiendo la posibilidad de aplicar los denominados números inocuos —*clean numbers*—, es decir, "PINs without having recourse to personal data" (Consejo de Europa, 1991: Concl. v), habría que ponderar si cumplen realmente el principio de adecuación aquellos códigos que introducen datos como el sexo o el origen geográfico de una persona. Finlandia, por ejemplo, atribuye los números impares a los varones y los pares a las mujeres.

16 Como señala el Tribunal Constitucional húngaro "personal number is the natural companion of all integrated record keeping systems... The power of a state administration... increases immeasurably" (sentencia 15-AB de 13 de abril de 1991, *Magyar Kozlony*, 30, 13 de abril de 1991, pp. 805-814; también en *www.privacy.org/pi/countries/hungary/hungarian_const_court_decision_id_numbers.txt* (6 de diciembre de 2001).

de la administración sin necesidad de recurrir a una generalización excesiva de los códigos.

Es cierto, por último, que las limitaciones a la intercomunicación de ficheros (artículo 11, LOPD) pueden reducir los riesgos, pero no llegan, en ningún caso, a anularlos.[17] Una vez admitido el código único y atendiendo a la omnipresencia de los instrumenros informáticos en la sociedad actual, no cabe considerar como remota la posibilidad de vulnerar esas garantías e interconectar los ficheros.[18]

17 La posibilidad de realizar cesiones de datos sin el consentimiento del afectado constituye, en este sentido, un impulso relevante a la implantación abusiva del mencionado código. La comunicación de datos requiere el "previo consentimiento del afectado" (artículo 11.1, LOPD), pero el segundo apartado de este mismo precepto incorpora diversas excepciones. No será necesario, por ejemplo, "cuando la cesión está autorizada en una Ley" [artículo 11.2, a), LOPD] o "cuando se trate de datos recogidos de fuentes accesibles al público" (artículo 11.2, b), LOPD). Por otra parte, el artículo 21.1 establecía que "los datos de carácter personal recogidos o elaborados por las administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos". El Tribunal Constitucional, en STC 292/2000, anuló el inciso destacado en itálica reduciendo, al menos en estos casos, las posibilidades de ceder datos sin la anuencia del afectado.
Martín Pallín no cree que pueda legitimarse "la interconexión de todos los ficheros de las administraciones públicas a través de un número único identificador" (1997, p. 83), pero debe tenerse en cuenta que el tenor literal de la ley no es tan tajante ya que no existe, siguiendo el ejemplo luso, una prohibición expresa del código individual. La aprobación de la directiva comunitaria despierta asimismo ciertas esperanzas. Martín Pallín reconoce que "no se ha abierto un debate comunitario sobre este problema, pero el espíritu y la letra de la directiva..., que se pronuncia decididamente en favor de las mayores garantías posibles..., permiten llegar a la conclusión de que el número único no es un procedimiento aceptable dentro de los parámetros garantistas en los que pretende moverse la directiva" (1997, p. 84).

18 Nos encontramos en "ámbitos en los que el mero progreso de la técnica sitúa al Estado en una posición que objetivamente pudiera resultar incontrolable tanto jurídicamente como de facto" (Souvirón Morenilla, 1994, p. 181). Se trata de una materia en la que los mecanismos jurídicos demuestran mucha fragilidad ya que "su ámbito subjetivo y objetivo es tan sumamente amplio que su total cumplimiento resulte, quizás, una utopía" (Vizcaíno Calderón, 2001, 26). Si eso es así, es todavía más acuciante analizar y, en su caso, eliminar cualquier factor que pudiera aumentar, sin justificación razonable, el poder ya de por sí considerable tanto de la administración pública como de los actores privados.
Tampoco cabe descartar la virtualidad de los mecanismos de autorregulación por los que los propios gestores de los códigos numéricos especifican las limitaciones de su

Llegados a este punto, resulta obligado preguntarse si las ventajas ofrecidas por el código universal son suficientes para considerarlo aceptable a la luz del principio de adecuación, es decir, si cabe considerar como *adecuada*, *pertinente* y no *excesiva* la exigencia de entregar el mismo código en un cúmulo de casos con finalidades variopintas. La respuesta no puede ser categórica. Analizando cada fichero deberemos decidir entre crear un codificación específica o usar claves ya existentes. En todo caso, tal opción deberá hacer hincapié en los argumentos expuestos. No podrá, en concreto, adoptarse sin una reflexión previa sobre sus consecuencias ni, circunscribiéndose a las finalidades de cada fichero, olvidar sus repercusiones globales.[19] El factor fundamental consiste en no contemplar al identificador numérico como un asunto exclusivamente organizativo, sino como un elemento potencialmente negativo para la eficacia de los derechos de las personas.

El Tribunal Constitucional español utilizó precisamente el principio de adecuación en la sentencia sobre el número de identificación fiscal. Destaca, en primer lugar, la trascendencia de los mecanismos preventivos establecidos por el propio ordenamiento ya

> que un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente inversor (*sic*) de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta (STC 143/1994, FJ 7).

Analiza posteriormente las exigencias derivadas de los textos internacionales y de la legislación española concluyendo que la normativa reguladora del NIF incluye las garantías suficientes: "la norma impugnada no legitima por sí misma la manipulación o difusión de datos que

uso. La *General Accounting Office* de Estados Unidos recuerda, en este sentido, la experiencia de 14 empresas que respondieron a "these concerns by... voluntarily executing a written agreement stating their intent to restrict disclosure of SSNs associated with data they obtain from nonpublic sources" (Us-Gao, 1999, p. 13).

19 La experencia nos muestra cómo, aunque los primeros pasos de un NIP estén circunscritos materialmente, resulta muy sencillo que vaya ampliando su radio de acción hasta convertirse *de facto* en un código único.

no esté estrechamente conectada con la finalidad que autoriza su recogida, y, en consecuencia, el recurso de amparo adquiere un carácter cautelar que le es impropio" (FJ 7).

No aborda, de forma expresa y directa, la equiparación entre NIF y DNI, pero alude a las garantías que, limitando la cesión de datos a otros archivos, impiden la distorsión de la finalidad concreta del fichero tributario. Se inclina, por lo tanto, por aceptar la existencia de un código común y confía en las cautelas previstas en el ordenamiento para evitar los riesgos de tal decisión.

VII. BIBLIOGRAFÍA

ALEGRE MARTÍNEZ, Miguel Ángel (1996) *La dignidad de la persona como fundamento del ordenamiento constitucional español*, León, Universidad de León.

APARICIO SALOM, Javier (2000) *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Pamplona, Aranzadi.

APDCM (2001), *Memoria 2000*, Madrid, Agencia de Protección de Datos de la Comunidad de Madrid.

CASTELLS, Manuel (2001) *Internet, llibertat i societat: una perspectiva analítica*, Barcelona, Internet Interdisciplinary Institute-IN3-Universitat Oberta de Catalunya.

www.uoc.es/web/cat/launiversitat/inaugural01/intro_conc.html, 16 de diciembre de 2001.

(2001a) *La galaxia Internet (Col. "Areté"), Barcelona, Plaza & Janés.*

CLEMENT, Andrew (2001), *National Identification Schemes (NIDS) and the Fight against Terrorism: Frequently Asked Questions*, Computer Professionals for Social Responsibility, Palo Alto-CA, versión 1.2.

www.cpsr.org/program/natlID/natlIDfaq.html, 23 de diciembre de 2001.

Consejo de Europa (1991), *The Introduction and Use of Personal Identification Numbers: the Data Protection Issues*, Estrasburgo, Committee of Experts on Data Protection-European Committee on Legal Co-operation-Council of Europe.

www.legal.coe.int/dataprotection/Default.asp?fd=pub&fn=PinsE.htm, 7 de diciembre de 2001.

DAVIES, Simon (1996), *Identity Cards. Frequently Asked Questions*, Privacy International, www.privacy.org/pi/activities/idcard/idcard_faq.html, 5 de diciembre de 2001.

Epic-Electronic Privacy Information Center (2001) *National ID Cards*, Electronic Privacy Information Center
www.epic.org, 24 de diciembre de 2001.

GABB, Sean (1999), *Identity Cards and the Total Surveillance Police State that Modern Technology Enables. A warning*, Londres, The Victoria Press.

www.jadis.demon.co.uk/books/idcards.pdf, 24 de diciembre de 2001.

GARFINKEL, Simson L. (1995), "Risks of Social Security Numbers", *Communications on the ACM*, 38-1, p. 146.

simson.net/clips/index.ACM.1995.html (16 de diciembre de 2001).

GAY FUENTES, Celeste (1995), *Intimidad y tratamiento de datos en las Administraciones públicas*, Madrid, Universidad Complutense.

HIBBERT, Chris (2001), *History and Significance of the Social Security Number*, Palo Alto-CA, Computer Professionals for Social Responsibility.

www.cpsr.org/cpsr/privacy/ssn/SSN-History.html, 15 de diciembre de 2001.

HOME OFFICE (1995), *Identity Cards A consultation Paper*, Cm 2879, Government's Consultation Paper.

LUCAS MURILLO DE LA CUEVA, Pablo (1990) *El derecho a la autodeterminación informativa* (Col. "Temas Clave de la Constitución española"), Madrid, Tecnos.

MARINA, José Antonio y VÁLGOMA, María de la (2000), *La lucha por la dignidad. Teoría de la felicidad política, (Col. "Argumentos"), Barcelona, Anagrama*.

MARTÍN PALLÍN, José Antonio (1997), "Constitucionalidad del número de identificación único", Agencia de Protección de Datos, *Jornadas sobre el derecho español de la protección de datos personales*, Madrid, Agencia de Protección de Datos, pp. 55-90.

MARX, Gary T. (2001), "Identity and Anonymity: Some Conceptual Distinctions and Issues for Research", en Caplan J./Torpey, J., *Documenting Individual Identity*, Princeton University Press.

web.mit.edu/gtmarx/www/identity.html, 17 de diciembre de 2001.

MCDONALD, Scott (1999), *Frequently Asked Questions Regarding Objections to Using Social Security Numbers for Identification*, SCAN-Sovereign Citizens Against Numbering.
www.networkusa.org/fingerprint/page6/fp-ssnfaq.htm, 20 de diciembre de 2001.
Privacy International (2001), *National ID Cards*, Privacy International.
www.privacy.org/pi/activities/idcard/, 23 de diciembre de 2001.
SOUVIRÓN MORENILLA, José María (1994), "En torno a la juridificación del poder informativo del Estado y el control de datos por la Administración", *Revista vasca de administración pública*, pp. 121-187.
Us-Gao United States General Accounting Office (1999), *Government and Commercial Use of Social Security Number is Widespread*, Report to the Chairman-Subcommitte on Social Security-Committee on Ways and Means-House of Representatives, GAO/HEHS-99-28.
www.networkusa.org/fingerprint/page2/fp-gao-ssn-report-99028.pdf, 18 de diciembre de 2001.
TWIGHT, Charlotte (2001), *Watching you: Systematic Federal Surveillance of Ordinary Americans* (Col. "Briefing Papers" 69), Cato Institute.
www.cato.org/pubs/briefs/bp69.pdf, 15 de diciembre de 2001.
VALERO TORRIJOS, Julián y LÓPEZ PELLICER, José Antonio (2001), "Algunas consideraciones sobre la protección de los datos personales en la actividad administrativa", *Revista vasca de administración pública*, 59, pp. 255-286.
VIZCAINO CALDERÓN, Miguel (2001), *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid, Civitas.
WALLACE, Jonathan (1999), *Nameless in Cyberspace. Anonymity on the Internet* (Col. "Briefing Papers", 54), Cato Institute.
www.cato.org/pubs/briefs/bp54.pdf, 15 de diciembre de 2001.
WOLFE, Claire (1998), *I am not a Number!: Freeing American from I. D. State*, Port Townsend, WA, Loompanics Unlimited.