Protección de datos por los gobiernos: el caso de los documentos nacionales de identidad
28 de octubre de 2009

Conferencista: José Luis Piñar Mañas
Moderadora: Comisionada María Marván Laborde

María Marván Laborde:

En estos momentos existe en México una discusión importante, especialmente sensible, alrededor del tema de esta conferencia. Como sabemos, hay un proyecto de la Secretaría de Gobernación para elaborar un documento de identidad que sería obligatorio para todos los mexicanos.

Nuestro ponente de este día, el doctor José Luis Piñar Mañas, ha sido amigo del IFAI desde que la institución empezó a funcionar, en 2003. En ese entonces, él era director de la Agencia Protectora de Datos Personales en España. La generosidad de la Agencia y la del propio doctor Piñar Mañas nos han ayudado mucho a avanzar en lo que hoy día es en México la protección de datos personales, por lo menos los que están en manos del gobierno. Le hemos hecho innumerables consultas y siempre nos ha respondido con una gran generosidad.

Sobra decir que estamos frente a una verdadera autoridad en la materia, que se ha enfrentado no sólo a la parte teórica de lo que es un documento de identidad, sino también a la negociación política, que en España llevó a buen puerto la incorporación del documento de identidad electrónico.

José Luis Piñar Mañas

José Luis Piñar Mañas. Doctor en Derecho por la Universidad Complutense de Madrid; catedrático de Derecho Administrativo en la Universidad CEU San Pablo de Madrid, de cuya Facultad de Derecho ha sido decano. Director de la Agencia Española de Protección de Datos de 2002 a 2007; vicepresidente del Grupo Europeo de Autoridades de Protección de Datos de 2003 a 2007. En 2003 fue presidente fundador de la Red Iberoamericana de Protección de Datos. Como director de la Agencia Española de Protección de Datos formó parte del Comité de Coordinación para la Implantación del Documento Nacional de Identidad Electrónico, creado en diciembre de 2004. Es profesor honorario de la Universidad de Guadalajara, Jalisco, en México; ha sido profesor invitado en las universidades de Florencia, Bolonia, Pisa y Macerata, en Italia; Luciada de Lisboa; la Católica de la Plata, en Argentina; Rio Grande do Sul, en Brasil, y Sergio Arboleda, en Colombia. Recibió el Premio de Investigación San Raymundo de Peñafort, de la Real Academia Española de Jurisprudencia y Legislación. Ha sido miembro del consejo redactor de diversas revistas especializadas; es autor de numerosas publicaciones sobre el derecho de protección de datos y transparencia, y ha impartido numerosas conferencias sobre este tema en España, Europa, América y Australia.

Gracias al IFAI por darme la oportunidad de estar una vez más en México para tratar un tema de particular importancia. Un tema que, como decía la comisionada, en estos momentos se está discutiendo en México y que afecta directamente el derecho fundamental de la protección de datos de carácter personal.

En mi calidad de director de la Agencia Española de Protección de Datos tuve ocasión de formar parte del Comité de Coordinación de la Implantación del Documento Nacional de Identidad Electrónico en España. Este Comité estaba presidido por la vicepresidenta primera del gobierno y formaban parte de él representantes de los ministerios del Interior, de Justicia y de Hacienda, de numerosas instituciones de enorme importancia, porque el proyecto lo merecía.

Las observaciones que hizo la Agencia Española de Protección de Datos durante la implantación del Documento Nacional de Identidad (DNI) electrónico fueron prácticamente atendidas

en su totalidad. Hicimos observaciones que tenían que ver con la seguridad del manejo de los datos, así como con el principio de proporcionalidad y con el principio de finalidad. Quiero resaltar la sensibilidad que hubo acerca de la incidencia de un documento de tanta importancia y, me atrevería a decir, tan necesario, como es una cédula de identificación. La incidencia que tiene en la protección de datos fue atendida y comprendida de inmediato por quienes tenían la responsabilidad de implantar ese documento en España.

Creo que hay tres grandes vectores que inciden en los documentos nacionales de identidad. Son el derecho a la protección de datos, el derecho a la identidad y el derecho a la seguridad nacional. Este último se plasma en la obligación de mantener un nivel de seguridad nacional por parte de los poderes públicos.

A continuación me referiré a los documentos nacionales de identidad como un instrumento para garantizar la identidad y la seguridad, y más adelante me centraré en un tema capital: qué datos deben incorporarse a un documento de identidad, con una especial referencia a los datos biométricos, que es el gran debate en la actualidad; ¿hasta qué punto pueden o deben agregarse datos biométricos en los documentos de identidad y, en su caso, cuáles de ellos deben incorporarse para considerar que se respetan los derechos de las personas y fundamentalmente el derecho a la protección de datos, y el mismo derecho a la dignidad de las personas?

Para ello analizaré los distintos principios que configuran el derecho fundamental a la protección de datos, así como los derechos de los afectados en relación con los datos que sean incorporados a los documentos de identidad. Por último haré breves comentarios acerca de dos puntos esenciales: por un lado, la relación entre autoridades de protección de datos y documentos de identidad y, por el otro, la relación entre transparencia y documentos nacionales de identidad.

El derecho a la protección de datos es un derecho reciente, vinculado a la privacidad y la intimidad. Cuando hablo de privacidad no me refiero a la idea general de vida privada, sino a un concepto que se acuñó a finales del siglo XIX y que no es fácil de definir, como han advertido diversos autores. El propio Tribunal Europeo de Derechos Humanos ha señalado que dicho concepto es amplio y no es susceptible de una definición exhaustiva. Quizá ha sido en el campo de la psicosociología y de la filosofía donde más ímpetu se ha puesto en delimitar un concepto de privacidad.

Ellen Alderman es referencia obligada en este punto, donde también es casi lugar común hacer mención de Thomas Cooley, juez estadounidense, que en 1888 acuñó la famosa frase: *The right to be let alone,* el derecho a ser dejado solo. Dos años más tarde, Samuel Warren y Louis D. Brandeis publicaron su célebre artículo, tan citado como poco leído, en la *Harvard Law Review,* "The right to privacy". Por cierto, este artículo surgió de una vivencia personal, pues la esposa de Brandeis había tenido una experiencia delicada que afectaba su privacidad, y eso les motivó a escribir este texto magnífico, en el que muestran cómo la constante adaptación de las cosas a la realidad "ha inventado un nuevo derecho a la privacidad", *the right to privacy.*

De modo que todos, en palabras de Cooley, tenemos el derecho a ser dejados solos: tenemos derecho a estar solos. En este tema, Greta Garbo decía: "yo no quiero estar sola, yo quiero que me dejen estar sola", que es una cosa muy diferente. No hablamos de aislarnos de la sociedad, sino de que si en algún momento queremos estar solos podamos hacerlo sin injerencias de los entes privados y mucho menos del poder público.

Más adelante, Alan Westin acuñó un concepto capital que se ha venido utilizando hasta nuestros días: el autor estadounidense define la privacidad en términos de autodeterminación. Este concepto sería después utilizado por el Tribunal Constitucional Alemán en la famosa sentencia sobre el censo electoral del 15 de diciembre de 1983, que dio lugar a esa idea del derecho a la privacidad, el derecho a la protección de datos, el derecho a la autodeterminación informativa.

¿Cuál es la clave de esta idea? La clave está en el control, la idea del control es la clave de la privacidad, ocupa el papel central. Westin lo dice claramente; él es, en efecto, quien ha resaltado con más énfasis la importancia del control: la privacidad implica libertad para elegir qué se desea comunicar, cuándo y a quién, manteniendo el control personal sobre la propia información.

Se abre la privacidad como el derecho a controlar la información. Los estudios empíricos han demostrado que para el individuo ese control es capital; se ha constatado que quienes perciben que mantienen el control sobre el uso que se hace de sus datos tras haberlos facilitado a un tercero, sienten menos invadida su privacidad que quienes piensan que han perdido el control sobre ellos. (Cabe hacer notar que no me refiero al con-

trol sobre los datos, que es distinto, sino al control sobre el uso que se hace de los datos; es decir, no se trata de que nuestros datos no vayan a nadie, sino de que, si son utilizados por alguien, podamos mantener el control sobre el uso que se hace de ellos.) De hecho, la violación del derecho de una persona a controlar su esfera privada, sea ésta física o informativa, constituye el factor más importante para que se sienta invadida la privacidad. Para ello no es necesario que la información sea más o menos importante o sensible. Una persona puede hacer pública información que le afecte sin que por ello considere violada su privacidad. Pero si pierde el control sobre ella, si alguien se la apropia, entonces pensará que su intimidad ha sido violada.

Quien en alguna ocasión ha facilitado o ha permitido el acceso a su propia información, no por ello renuncia a su privacidad. El que yo esté haciendo pública información sobre mi persona no significa que esté consintiendo que con esa información cada cual haga lo que quiera. Yo debo mantener el control sobre mi información.

En este sentido, en México se ha producido recientemente un acontecimiento que todos conocemos, que es la aprobación de la reforma del artículo 16 constitucional. Merece la pena leer el nuevo párrafo segundo del citado artículo: "Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros". Esta modificación constitucional sin duda ha colocado a México a la cabeza de los países que reconocen con un alto nivel normativo y de forma clara, precisa y expresa el derecho fundamental de todos a la protección de sus datos personales. Éste es un precepto de extraordinaria importancia que debe condicionar enteramente cualquier proyecto normativo que a partir de ahora se acometa en este renglón en los Estados Unidos Mexicanos. Se convierte, así, por ejemplo, en el filtro a través del cual debe analizarse la implantación de una célula de identificación personal.

Las anteriores consideraciones tienen particular relevancia si hablamos de un proyecto que tiene como objeto esencial el manejo de datos personales que pueden incluir datos biométricos.

Por lo general tales datos se consideran dignos de especial protección o particularmente sensibles dado que afectan a la más interna y profunda intimidad de las personas. Por ello cualquier norma que afecte a los datos biométricos de las personas ha de ser rigurosamente respetuosa de la intimidad, de la protección de los datos de carácter personal.

Si esto es así, si estamos hablando de un derecho fundamental, es imprescindible que hagamos referencia a los principios que configuran el derecho fundamental a la protección de datos. En efecto, si hablamos de un derecho fundamental la cuestión estriba en determinar cuáles son los elementos que configuran ese derecho fundamental. ¿De qué derecho fundamental estamos hablando?

Partamos de algo sumamente importante: cuando hablamos de protección de datos de carácter personal estamos hablando, en primer término, de un poder de disposición, de un control sobre nuestros datos.

En segundo lugar, debemos tener muy claro que cuando alguien recoge datos de un tercero, éste nunca pierde la "propiedad" de sus datos. Los datos que se incorporan a un fichero, a una base de datos, son siempre y por definición datos ajenos, no son datos del propietario de la base de datos. Hay que distinguir entre continente y contenido; una cosa es la base de datos y otra la información que contiene esa base de datos. La información pertenece siempre al titular de los datos personales, porque de otra manera estaremos violentando el derecho a la protección de datos.

Recuerdo una vez que se dañó el disco duro de mi ordenador personal. En el taller de servicio me dijeron: "No se preocupe, se lo reparamos, tiene garantía". Cuando fui a recoger el equipo me dijeron: "Le hemos cambiado el disco duro, pero nos hemos quedado con su disco duro anterior". Y yo les dije: "No, eso no, en lo absoluto". E insistieron: "Se lo hemos cambiado, nos quedamos con su disco duro anterior". Entonces no había las técnicas actuales para copiar información. Les reiteré: "Me tienen que dar el disco duro, quizá sea suyo, pero la información es mía. Hagan ustedes lo que quieran, si lo desean, quédense con el continente, pero el contenido me lo dan". Como eso era imposible, me dieron el disco duro. Lo que yo quería decir era: "Miren, ustedes creen que el disco duro es suyo, con todo lo que tiene, pero esto no es así. La información que hay dentro es mía, ni siquiera es mía, es del

titular de los datos a los que se refiere la información que hay en este disco duro". Esto es sumamente importante y define el derecho a la protección de datos. Los datos siempre son de los titulares, nunca son de los dueños de las bases de datos.

Por otra parte, estamos hablando de un derecho que se refiere a datos incorporados a una base de datos, no a datos sueltos que no están sometidos a tratamiento (es la expresión técnica que se utiliza). Tratamiento es una expresión que hace referencia a la recopilación, manejo, uso, cesión, etcétera, de los datos. Si yo ahora hiciese pública una información, por decir algo, de la comisionada María Marván –que sería, sin duda, muy positiva y elogiosa–, no estaría violando la ley de protección de datos, sino otra legislación, la ley del derecho al honor, a la propia imagen, pero no a la protección de datos, porque no estoy utilizando una información reunida en una base de datos. Si yo tuviera una información de la doctora Marván en una base de datos mía y la facilitara, entonces ya sería otra cosa; ahí sí entraría la legislación de protección de datos.

Sin duda alguna las cédulas de identificación requieren de la creación de una base de datos. Ésta sería una de las más importantes bases de datos que puede tener un país y eso implica que se aplique la legislación de protección de datos a todo uso que se haga de esa información. Poder de disposición, control sobre los datos, datos ajenos, manejo o tratamiento de datos incorporados a bases de datos. Ante todo esto, ¿cuáles son los principios que configuran este derecho?

El primer principio es el de información. Si se recaba un dato, hay que informar al titular: "Mire usted, yo recabo sus datos y le tengo que decir lo que voy hacer con ellos, porque si no le informo eso, usted pierde el control". Si no le digo al interesado que sus datos los voy a ceder a una empresa o los voy a incorporar a un documento de identidad, ese individuo pierde el control sobre ellos. Ya veremos que en México estos principios derivan del artículo 16 constitucional y están recogidos en la Ley Federal de Transparencia y Acceso a la Información Pública y también en los lineamientos de protección de datos que ha emitido el IFAI.

El segundo principio es que el tratamiento, el manejo de los datos, debe estar amparado en un título que habilite su utilización porque la ley lo establece o porque hay consentimiento, pero no se pueden recabar datos sin legitimación. Este dato lo encuentro y lo incorporo

a un fichero. ¿Por qué? O la ley lo permite o hay consentimiento o hay una razón contractual, tiene que haber un título habilitante, esto es importantísimo.

Los siguientes principios se refieren a que los datos deben ser proporcionales a la finalidad que se persigue, ni más ni menos, y, sobre todo, nunca deben ser más de los estrictamente necesarios. Sólo se deben recoger los datos necesarios para la finalidad perseguida, deben ser adecuados, pertinentes, no excesivos para la finalidad que se pretenda. Tanto el principio de proporcionalidad como el de finalidad son esenciales y poseen especial trascendencia en las cédulas nacionales de identidad.

Otro principio es el de seguridad. Los datos tienen que ser manejado con seguridad, con total seguridad. De qué me sirve decir o pensar o creer que tengo el control sobre mis datos, si se los facilito a alguien, y éste los va a tratar de modo que cualquiera va a poder acceder a ellos sin que haya ninguna consecuencia derivada de ese uso o acceso ilegítimo. Además, si no hay medidas de seguridad a lo mejor ni siquiera el titular del fichero se entera de que ha habido un acceso sin control a sus datos de carácter personal. Por tanto, los datos tienen que tratarse con absoluta seguridad.

El último principio es el de control independiente. Si ven todos los principios anteriores, se darán cuenta de que parten del control sobre los propios datos personales: información, consentimiento, proporcionalidad, finalidad, seguridad. Si alguno de estos principios cede o se viola, se viola el propio derecho, porque si se viola el principio de seguridad o el del consentimiento o el de finalidad se está perdiendo el control sobre los propios datos.

Si alguien me dice que va a utilizar los datos para una finalidad y en realidad los emplea para otra, pierdo el control: ya no sé qué pasa con mis datos. Esto genera desconfianza, lo cual es muy grave, porque además –y esto es algo también muy importante– las violaciones del derecho fundamental a la protección de datos pasan inadvertidas; eso es algo que caracteriza peculiarmente a este derecho. Si a mí me roban el saco o el bolígrafo, me entero de inmediato; a lo sumo cuando voy a buscar el saco o el bolígrafo, pero me entero. En cambio, si alguien me roba mis datos a lo mejor no me entero nunca y no estaré consciente de las consecuencias derivadas del mal uso que se ha hecho de mis datos de carácter personal.

Les pongo un ejemplo. En Brasil, en aras de la transparencia, pero en mi opinión de una transparencia no del todo bien entendida, se hicieron públicas todas las sentencias judiciales; entre otras, las sentencias de los tribunales de lo laboral, de lo social. Esto permitió que varias empresas especializadas hicieran una base de datos con los nombres de todos los trabajadores que habían sido despedidos o que habían obtenido la victoria frente a la empresa en algún litigio laboral o que simplemente habían entrado en conflicto con el patrón. Hubo un momento en el que un empresario no contrataba a nadie sin antes consultar esa base de datos de los trabajadores que habían tenido problemas con las empresas ante los tribunales. Claro, las personas que no eran contratadas nunca supieron que el rechazo se debía a que alguien había hecho un uso ilegítimo de sus datos. Por eso hay que ser muy cuidadosos con el derecho a la protección de datos. Repito, porque las violaciones de este derecho pasan inadvertidas.

Para tutelar el principio de control independiente debe haber una autoridad independiente, y no porque esto sea el modelo europeo –muchas veces se dice: "claro, es que éste es el modelo europeo, el de la directiva de protección de datos que se quiere implantar"–, sino porque hay una resolución –la 45/95 de la Asamblea General de Naciones Unidas, del 14 de diciembre de 1990, cuyo punto octavo dice: "El derecho de cada país designará a la autoridad que, de acuerdo con su sistema jurídico interno, vaya a ser responsable de supervisar la observancia de los principios arriba establecidos [de protección de datos]. Esta autoridad ofrecerá garantías de imparcialidad, independencia frente a las personas o agencias responsables de procesar y establecer los datos, y competencia técnica". Es decir, es la Asamblea General de Naciones Unidas la que ha dicho, en 1990, que deben existir autoridades independientes de tutela y garantía del derecho a la protección de datos.

En Europa así ocurre. El artículo octavo de la Carta de los Derechos Fundamentales de la Unión Europea insiste en la necesidad de que el respeto a las normas de protección de datos quede sujeto al control de una autoridad independiente. Debo decir que se presume que si falta esa autoridad, no es posible, en ningún caso, considerar aceptable el marco jurídico regulador del derecho a la protección de datos. Uno de los puntos esenciales de las decisiones de adecuación que hasta ahora ha aprobado la Comi-

sión Europea en relación con la protección de datos que ofrecen terceros países es precisamente la existencia de una autoridad independiente de control.

Me referiré ahora al derecho a la identidad, que se reconoce ya en el artículo sexto de la Declaración Universal de Derechos Humanos: "Todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica". Por tanto, la identidad personal es un derecho de todo ciudadano y los Estados tienen la obligación de establecer los mecanismos adecuados para facilitársela. Además, otorgar identidad a las personas adquiere una nueva dimensión cuando se trata de establecerla para un uso no presencial en medios telemáticos, y aunque la identidad sea siempre física, es necesario establecer mecanismos y procedimientos electrónicos para verificarla en estos nuevos ámbitos.

Bogotá ha resaltado con claridad la relación entre derecho a la identidad y protección de datos, pues considera que la identidad es más que la suma de la información que nos afecta; es un proceso que exige no sólo el derecho al olvido individual, sino, sobre todo, que el conjunto de nuestros datos personales no esté disponible o, al menos, que no lo utilicen los demás. Esto nos sitúa, en mi opinión, en el centro del debate.

Existe un derecho a la identidad que exige, para ser plenamente efectivo, que nuestros datos personales no estén disponibles o no sean utilizados. La disponibilidad y la utilización sólo se permitirán cuando haya una habilitación precisa para una finalidad determinada y legítima, y sólo se incluirán los datos imprescindibles para ello.

En este sentido, uno de los problemas más graves que se plantea en la actualidad en relación con este tema es el robo de identidad. Se trata, con toda seguridad, de la consecuencia más seria derivada del uso ilegítimo de los datos de carácter personal. Nos arrebatan, aunque sea sólo de manera temporal o momentánea, nuestra identidad personal, que se utiliza sin que estemos conscientes de ello. Por ejemplo, cuando alguien se hace con nuestros datos bancarios, nos desdoblamos: somos nosotros y otro diferente. ¿Por qué? Porque alguien está usurpando nuestra identidad, alguien está utilizando nuestra tarjeta de crédito y no somos nosotros, sino es él, quien actúa en nuestro nombre; nos ha robado la identidad. Otro actúa como si

fuésemos nosotros, pero sin serlo. Esto no es en absoluto ciencia ficción, al contrario, se trata de una de las situaciones más recurrentes en estos días. De hecho, está demostrado que el comercio electrónico tiene ante sí un enorme reto, que es el de la desconfianza que existe a la hora de facilitar datos personales por Internet.

Por eso es imprescindible establecer sistemas que garanticen la identidad cierta de las personas, a fin de evitar o disminuir los riesgos de robo de identidad.

Uno de los sistemas más generalizados es el que se basa en la utilización de datos biométricos. El Grupo Europeo de Autoridades de Protección de Datos, del que tuve el honor de ser vicepresidente, elaboró en agosto del 2003 un documento muy interesante sobre biometría, el documento de trabajo número 80. En él se dice que los sistemas biométricos son aplicaciones de las tecnologías biométricas que permiten la identificación de las personas. Cada biometría depende más o menos del elemento en cuestión; el elemento biométrico es permanente y distintivo de cada persona. Los sistemas de identificación biométrica se aplican con cierta normalidad, aunque plantean algunos problemas, que veremos más adelante.

Por último, en lo que respecta al derecho a la seguridad, prácticamente todos los textos internacionales y constitucionales reconocen el derecho a la seguridad de las personas. Todos tenemos derecho a la seguridad, a que los poderes públicos adopten las medidas necesarias para garantizar nuestra seguridad, sobre todo tras los terribles atentados del 11 de septiembre y los que luego se produjeron en Madrid en 2004, en Londres en 2005, y tantos otros que han ocurrido, desgraciadamente, con posterioridad.

Los Estados, por tanto, tienen la obligación de adoptar las medidas dirigidas a proteger a los ciudadanos frente a la inseguridad. Ahora, esos peligros deben ser reales, no imaginarios, por un lado, y por otro, las medidas deben ser necesarias y amparadas por la ley. Sólo una ley puede establecer restricciones a los derechos de las personas en aras de la seguridad. Las medidas que se adopten tienen que ser, en todo caso, respetuosas de los derechos fundamentales. Porque si en algún momento se aplican medidas que restrinjan de manera ilegítima los derechos fundamentales, estaremos dando la victoria a quien atenta con-

tra nuestra seguridad. Ésa será su primera y gran victoria: conseguir que se limiten los derechos de los ciudadanos en aras de la seguridad.

Debo decir que hasta hace poco tiempo se habían adoptado medidas, a escala global o nacional, que afectaban el derecho a la protección de datos, no tenían mucha justificación y se amparaban en la generación de un ambiente de inseguridad que no siempre se sustentaba sobre bases reales.

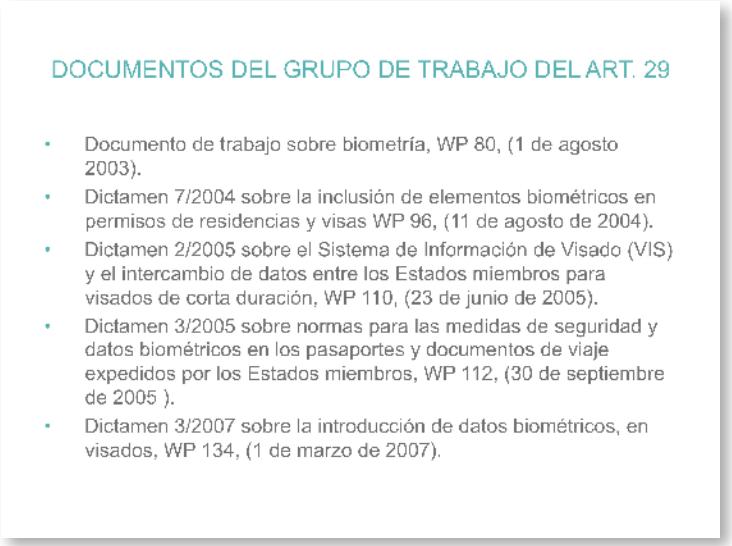
En este sentido, quiero recordar una frase que pronunció el presidente Barack Obama en su discurso de toma de posesión el 20 de enero del 2009: "En cuanto a nuestra defensa común, rechazamos como falso que haya que elegir entre nuestra seguridad y nuestros ideales". Ésta es la clave: no se puede renunciar a los derechos fundamentales en aras de la seguridad.

Éstos son los términos del debate y ahí es donde encaja el documento de identidad, el cual debe ser, en México y en cualquier país, personal e intransferible; debe ser emitido, evidentemente, por los poderes públicos, y debe gozar de la protección que las leyes otorgan a los documentos públicos y oficiales. Su titular debe estar obligado a su custodia y conservación. ¿Para qué sirve? Fundamentalmente para acreditar la identidad y los datos personales de su titular.

En muchas ocasiones, además, garantiza o acredita la identidad no sólo física, sino también electrónica. Muchos documentos de identidad se están incorporando a la función de la firma electrónica, de identificación electrónica; el DNI español, por ejemplo, ya incorpora la firma electrónica, de modo que tiene una doble función: la función de identificación y la de firma electrónica.

Hay que decir que cada vez es más usual incorporar datos biométricos a los documentos nacionales de identidad, lo cual plantea no pocos problemas. El Grupo de Trabajo del Artículo 29 sobre Protección de Personas, de la Comisión Europea, ha emitido diversos documentos muy importantes en relación con la utilización de datos biométricos en documentos de identidad, en pasaportes, en visados. A continuación me referiré a algunas de sus conclusiones.

En la Conferencia Internacional de los Comisarios de Protección de Datos y de la Privacidad, que se efectuó en Montreux en 2005, donde participó el IFAI, se adoptó una resolución sobre el uso de la biometría en pasaportes, tarjetas de identidad y documentos



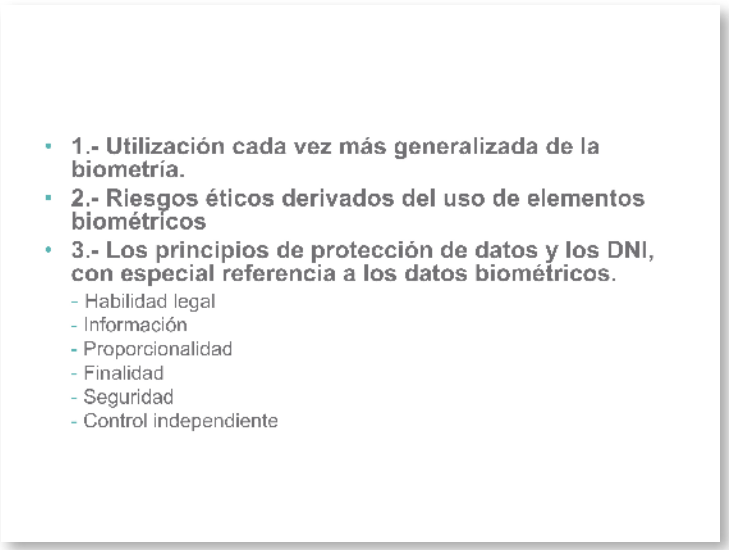
de viaje. En esta resolución se hizo hincapié en que tienen que adoptarse garantías eficaces en las primeras fases de implantación de un documento de identidad. Eso es clave, esencial.

Cuando se pone en marcha un documento de identidad hay que implementar garantías eficaces, rigurosas. Además, deben respetarse los principios que hemos mencionado; sobre todo, los principios de proporcionalidad y de finalidad. El Grupo de Trabajo del Artículo 29 hace referencia a esa utilización cada vez más generalizada y llama la atención acerca del uso de datos biométricos que pueden afectar a la dignidad de las personas, por lo cual tienen que utilizarse con absoluto rigor.

Dicho grupo señala: "Anteriormente el uso de la biometría estaba limitado sobre todo a los ámbitos del ADN y la comprobación de las huellas digitales. La recopilación de las huellas digitales se utilizaba especialmente para fines legales (por ejemplo investigación criminal). Si la sociedad fomenta el desarrollo de bases de huellas digitales u otras bases de datos biométricos para diversas aplicaciones habituales, se puede incrementar la reutilización potencial de estos datos por parte de otros como elemento de comparación e investigación...". El Grupo de Trabajo del Artículo 29 dice que entre estos "otros" que pueden reutilizar la información se hallan las autoridades encargadas de emitir esos documentos. Hay unos riesgos éticos evidentes derivados

del uso de los datos biométricos. Se han realizado estudios que llaman la atención acerca del empleo de estos datos que puede afectar la dignidad de una persona y, no hay que olvidarlo, siempre se tiene que respetar la privacidad y la intimidad.

En este sentido, ¿qué principios deben siempre tenerse en cuenta? En primer lugar, la habilitación legal. Debe haber una ley que permita la incorporación de datos biométricos a los documentos de identidad. El artículo 16 constitucional mexicano, que cité antes, debe ser el parámetro de la ley que permita la incorporación de datos biométricos. No es necesario el consentimiento personal; con o sin consentimiento hay que facilitar los datos que el legislador decida que se incorporen a los documentos de identificación.



Cosa distinta es la cesión de estos datos. En este caso sí se requerirá consentimiento para cualquier uso distinto que se pretenda hacer de los datos biométricos incorporados a los documentos de identidad. Hay que respetar el principio de información y hacer saber a todos los afectados qué se va a hacer con sus datos. Cuando se recaben datos para incorporarlos al documento de identidad, hay que informarlo. Es algo que, por lo demás, se recoge en la legislación de protección de datos. Pero, sobre todo, es imprescindible respetar los principios de proporcionalidad, finalidad y seguridad.

Sin duda, los principios más importantes en relación con el tratamiento de datos de los documentos de identidad y, en particular, de los datos biométricos, se deriva de la calidad del dato, que, en definitiva conduce a cumplir con los principios de proporcionalidad y finalidad. El Grupo de Trabajo del Artículo 29 ha dicho que el cumplimiento de este principio implica una determinación clara de los fines para los que se recogen y emplean los datos biométricos. Además, deben ser datos proporcionales.

En este sentido, no conozco ningún documento de identidad que incorpore más datos biométricos que la imagen facial, la firma –si es que se puede considerar dato biométrico– y las huellas dactilares. Incluso, el Grupo de Trabajo del Artículo 29 ha reconocido la proporcionalidad de recabar diez huellas dactilares, pues cada vez es más fácil falsificar las huellas o que haya errores con respecto a ellas. Esto es lo que se suele utilizar; no conozco ningún documento de identidad que incorpore más datos biométricos que éstos. En algunas ocasiones se discute la posibilidad de incorporar el iris, pero, sinceramente, no conozco ningún caso en el que se incluya el registro de esta parte del ojo.

Se puede plantear que es desproporcionado incorporar tantos datos biométricos. De lo que se trata es de identificar con certeza a la persona, siempre bajo el prisma del principio de minimización de datos. Para esta finalidad, hay que optar por la solución menos intrusiva para los derechos fundamentales. Y si con unos datos personales equis se tiene la certeza de la identificación, entonces no hace falta pedir más datos. Se ha dicho que los datos biométricos pueden ser necesarios porque son los únicos que pueden garantizar la identificación. Quizá sea así, pero nunca se deben pedir más de los necesarios.

En cuanto al principio de seguridad, debo señalar que el sistema entero de documentos de identidad depende en gran medida de él. Si por cualquier motivo se produce un fallo en la seguridad, si llega a haber una cesión no consentida de datos, una venta de datos, toda la confianza en el sistema se viene abajo. Si se pueden falsificar datos, si se pueden falsificar documentos de identidad, si se pueden falsificar informaciones, el sistema ya no cumple con su finalidad, que era la identificación cierta y precisa del titular. Por eso es necesario tener un entorno seguro en el manejo de los datos. El Grupo de Trabajo del Artículo 29 indica que es imprescindible contar con personal completamente fiable

y con la formación adecuada, incluida la sensibilidad en materia de protección de datos. Además, se debe evitar a toda cosa la posibilidad de recurrir a prestadores de servicios externos.

Por otro lado, hay que reconocer los derechos de los afectados, los derechos de acceso, de rectificación, cancelación y oposición, sin perjuicio de que en ocasiones no es posible el derecho de cancelación ni el derecho de oposición; pero, por supuesto, sí el derecho de acceso y el de rectificación.

En cuanto a la transparencia de los derechos de los afectados, debe existir una autoridad de control de protección de datos. Aquí hay que distinguir muy claramente quién es competente para perseguir un uso ilegítimo de los documentos de identidad. Por ejemplo, la falsificación de documentos se perseguiría por la vía penal, y quien es competente en este caso –así lo entiendo, y lo dice también el Grupo de Trabajo del Artículo 29–, debe ser la autoridad con competencia en materia de protección de datos.

Finalmente, la transparencia de los documentos de identidad es imprescindible en una sociedad transparente para garantizar la identidad de las personas y su identificación segura. Pero la transparencia no puede ser excusa para acceder a información que permita manipular la información identificadora. ¿Es permisible acceder a los números de identificación, a los datos biométricos, a los datos que definen la identidad? En mi opinión, eso implicaría acceso a datos personales, los más personales de todos, aquellos que nadie más tiene y que nos diferencian de los demás, los que junto con otra información configuran nuestra identidad única y diferenciada. Por eso, nadie más que el interesado y quien esté legalmente habilitado para ello pueden tener acceso a esos datos; nadie, ni siquiera en aras de la transparencia, salvo los habilitados, puede tener acceso a nuestra identidad, ya que de otro modo se abrirían las puertas al robo de identidad.

El acceso a la información, en suma, no puede implicar el acceso a la identidad personal. En definitiva, de lo que se trata es de respetar la protección de datos.

Para terminar, discúlpenme si me tomo el atrevimiento de parafrasear nada menos que a Benito Juárez, pero creo que la clave está en: "El respeto al dato ajeno es la paz".

Nada impide que haya una sola identificación, pero esta cédula de nada serviría –y créanme que es así– si por cualquier motivo

no cumple su finalidad y no se satisfacen las exigencias de respeto a los derechos y de seguridad que deben ir aparejadas con la implantación de algo tan importante como es un documento público que acredita nuestra identidad única e irrepetible.

Muchas gracias.

Respuestas a las preguntas de la audiencia

María Marván Laborde: Hay que resaltar la importancia que tiene el uso cuidadoso de datos biométricos; sin lugar a dudas su empleo creciente obliga a que se incremente la responsabilidad, así como las medidas de seguridad en su manejo. Para ello, hay análisis específicos de impacto a la privacidad. Vale la pena decir –porque algunas de las preguntas se refieren a eso– que el IFAI es la autoridad en protección de datos personales en manos del gobierno federal y, por lo tanto, como autoridad tendría mucho que decir respecto del documento nacional de identidad que pretende poner en marcha la Secretaría de Gobernación, de modo que trabajaremos con ella. Nuestro aval podría darse sólo si se cumple con las condiciones que como autoridad haya puesto el IFAI, lo cual no ha ocurrido hasta ahora.

Una de las cuestiones indispensables es la necesidad de generar confianza en la institución responsable de guardar estos datos y la seguridad que tenga el dueño de los datos de que éstos no serán usados por otra agencia, aun cuando ésta fuese también un organismo gubernamental.

José Luis Piñar Mañas: Algunas de las preguntas tienen que ver con el DNI en España. Desde el momento en que se constituyó el Comité de Coordinación para la Implantación del DNI Electrónico, yo acudía como representante de la Agencia Española de Protección de Datos; además, se constituyeron otros comités técnicos de los que formaban parte miembros de la agencia, técnicos informáticos, matemáticos. La verdad es que al principio había ciertas reticencias hacia nosotros y los demás participantes pensaban que íbamos a poner obstáculos, pero al final fueron muy receptivos. Por ejemplo, cuando se puso en marcha el DNI electrónico, que incorporaba un chip con una gran capacidad de almacenamiento de información, algunos pretendieron que se agregara a ese chip mucha más información que la que el DNI electrónico requería. La agencia, entonces, dijo: "Ojo, eso no es una cédula de identificación, eso es otra cosa". La finalidad es la identificación, luego, sólo se pueden incorporar datos de identificación, no otros.

Hubo otro punto en el que nuestra opinión tuvo un peso importante. Se pretendía que se utilizase para la lectura de la información un sistema de radiofrecuencia –RCID, Resistive Capacitive Identification – y dijimos que no. Porque la radiofrecuencia, que es quizá lo más avanzado en estos momentos, es mucho más arriesgada desde el punto de vista de la protección de datos; en cambio, es mucho más segura la lectura de información por contacto, por un microchip de contacto. Y así se hizo.

Quiere decir que fueron propuestas que consideraban los principios de proporcionalidad, finalidad y seguridad, y que fueron tomadas muy en cuenta.

En cuanto a si es mejor el iris que las huellas dactilares para identificar con certeza, se considera que hoy es mucho más seguro el iris que las huellas dactilares, pues éstas tienen un margen de error, no así el iris. Lo que quizá iría más allá del principio de proporcionalidad es exigir tantos datos biométricos. Eso sí, cuantos más datos biométricos se exijan, más medidas de seguridad hay que implantar. Cuanta más información tiene un documento de identidad, más medidas de seguridad hay que establecer y quizá ni así se compense. Eso se planteó en España: a lo mejor no se compensaban unas medidas de seguridad derivadas del uso de una información que no se consideraba necesaria para la finalidad que se perseguía.

Juan Carlos Castillo, de Tabasco, pregunta: ¿cómo se establece el grado de responsabilidad del servidor público que otorga datos personales de un tercero, sin consentimiento del titular? Ésta es una infracción clarísima, una violación al derecho a la protección de datos; es una cesión de datos sin consentimiento. Dependerá de cada país establecer la responsabilidad. Pero si se demuestra quién ha sido el que adquirió los datos, se podrá exigir responsabilidad.

Éste es un tema que también nos lleva a hablar de las medidas de seguridad. Se tienen que establecer las medidas de seguridad suficientes de modo que se pueda identificar exactamente quién ha accedido a qué datos para que éste deba, en su caso, justificar por qué ha tenido acceso a esos datos. Si resulta que hay una fuga de información de la célula de identificación y nadie sabe a quién se debe esa fuga, ni cuándo ha sucedido, ni por qué, va a ser imposible exigir responsabilidades. Por eso deben establecerse medidas de seguridad muy rigurosas.