

Tecnologías de Información y Comunicación en la Administración Pública: Conceptos, Enfoques, Aplicaciones y Resultados

J. Ramón Gil-García

J. Ignacio Criado

Juan Carlos Téllez

(Editores)



Infotec

Dirección Ejecutiva (DE)

Dr. Sergio Carrera Riva Palacio

Dirección Adjunta de Innovación y Conocimiento (DAIC)

Dr. Juan Carlos Téllez Mosqueda

Dirección Adjunta de Competitividad (DAC)

Dr. Armando Peralta Díaz

Dirección Adjunta de Desarrollo de Software (DADS)

Mtro. Luis Humberto Alva Martínez

Dirección Adjunta de Administración (DAA)

Lic. Hilda Georgina Méndez Lozoya

*Tecnologías de Información y Comunicación en la Administración Pública:
Conceptos, Enfoques, Aplicaciones y Resultados*

© Jose Ramon Gil García, Juan Ignacio Criado, Juan Carlos Téllez Mosqueda
(Editores)

Primera edición: abril, 2017

ISBN: 978-607-7763-24-6

D.R. © INFOTEC Centro de Investigación e Innovación en Tecnologías
de la Información y Comunicación

Av. San Fernando No. 37 Colonia Toriello Guerra

Delegación Tlalpan, C.P. 14050 México, Ciudad de México

México, MMXV

www.infotec.mx

Prohibida la reproducción total o parcial, de la obra, sin la autorización por escrito
de INFOTEC

Impreso en México/Printed in México

Capítulo 5

Seguridad, tecnología y Administración Pública electrónica: La necesaria reconfiguración del alcance de las garantías jurídicas ante la innovación tecnológica

Julián Valero

Universidad de Murcia, España

julivale@um.es

Resumen

En el ámbito de la Administración electrónica la eficacia de las normas jurídicas depende en última instancia de la efectiva aplicación de las garantías tecnológicas y, en definitiva, de las medidas de seguridad que procedan en función de la naturaleza de la información que se trate y de la necesidad de garantizar su autenticidad e integridad. Sin embargo, no basta con el mero establecimiento de tales requisitos sino que, asimismo, resulta imprescindible asegurar su cumplimiento en la práctica. A tal efecto las normas deben estar adaptadas a la realidad tecnológica en la que deben ser aplicadas. También es preciso que la intensidad de las consecuencias jurídicas que se derivan de los supuestos de incumplimiento sea proporcionada a la gravedad de la infracción. En este trabajo se ofrece una interpretación de las categorías e instituciones generales que se ven afectadas en los proyectos e iniciativas de modernización tecnológica de las Administraciones Públicas desde la perspectiva del valor jurídico de las medidas de seguridad. En este sentido, se propone la creación de estructuras de control adecuadas y, asimismo, el establecimiento de medidas que permitan garantizar el cumplimiento de los estándares tecnológicos de seguridad; en última instancia, se llega incluso a contemplar la interrupción de los servicios en los supuestos de mayor gravedad. Finalmente, se insiste en la necesidad de ampliar el alcance del derecho de acceso a la información reconocido a los ciudadanos en sus relaciones con las Administraciones Públicas a fin de que no sólo tenga por objeto los datos en poder de estas últimas sino, asimismo, los tratamientos informativos que realicen y las condiciones técnicas en que tienen lugar.

Palabras clave: e-Administración, medidas de seguridad, derechos del ciudadano, innovación tecnológica, seguridad jurídica

Abstract

The effectiveness of legal norms in the field of eGovernment depends in the last analysis on the real application of technological safeguards and, ultimately, of the adequate security measures according to the kind of information concerned and the need to ensure its authenticity and integrity. However, not only is it important establishing such requirements from a theoretical perspective but also to ensure its

compliance in practice as well. It is also necessary that the intensity of the legal consequences arising from the events of default is proportionate to the importance of the infringement. In this paper we offer an interpretation of categories and general institutions that are involved in those projects and initiatives related to technological modernization of public bodies from the perspective of legal value of security measures. In this regard, the establishment of adequate control structures and the enactment of legal measures to ensure the respect of technological safety standards; as a last resort, we even propose the interruption of those services affected in the most serious cases. Finally, we stress the need to expand the scope of the right of access to the information by citizens in their relationships with public bodies so that its object is enlarged from data to their processing and the technical conditions in which they take place.

Keywords: e-Government, security measures, citizen's right, technological innovation, legal certainty

1. El problema de fondo

En el actual desarrollo de la tecnología, la creciente innovación en el ámbito de los servicios públicos implica que las garantías jurídicas estén pasando a un segundo plano para facilitar su potencial innovador o, incluso, estén sirviendo en otros casos para justificar la aparición de barreras y dificultades basadas en la desconfianza por parte de los operadores jurídicos. En consecuencia, resulta preciso reforzar el efectivo cumplimiento de las normas técnicas, tanto las previstas en las normas jurídicas como las que, en su caso, pueda considerarse un adecuado estándar por parte de la industria. De lo contrario existe un riesgo cierto de que el proceso de modernización tecnológica de la actividad de los poderes públicos y, asimismo, de las comunicaciones con la ciudadanía se impulse a costa del efectivo cumplimiento de las normas técnicas y, por tanto, de la seguridad jurídica en la que ha de descansar la confianza imprescindible para el respecto de todos los bienes e intereses en juego.

Hasta el momento la discusión doctrinal se ha centrado en aspectos concretos necesarios para la articulación del sistema en su conjunto desde la perspectiva de sus implicaciones tecnológicas, tal y como ha sucedido con la interoperabilidad (Gamero, 2009: 292 y ss.), la firma electrónica (Alamillo,

2012: 419 y ss.), la singular incidencia de la protección de los datos personales (Valero, 2013: 392 y ss.), la automatización de la actuación administrativa (Martín, 2009: 353 y ss.; Alamillo y Uríos, 2011), la neutralidad tecnológica (Boix, 2007) o el control sobre el funcionamiento de las aplicaciones (Palomar, 2007, 90). Sin embargo, al margen de las reflexiones que se recogen en obras generales (Martínez, 2009), no ha tenido lugar un debate específico sobre las implicaciones jurídicas de la tecnología en el ámbito de las Administraciones Públicas. A tal efecto no basta con subrayar la necesidad de que estas últimas deban modernizarse teniendo en cuenta los avances tecnológicos sino que, además y sobre todo, resulta imprescindible llevar a cabo una reconsideración conceptual de las herramientas y paradigmas propios del Derecho Administrativo (Piñar, 2011: 26). Ahora bien, pretender una regulación exhaustiva, completa y sistemática de los aspectos tecnológicos por parte de las normas jurídicas resulta cuando menos ilusorio e ingenuo (Esteve, 1999: 27), de manera que nuestro análisis se centrará únicamente en aquellos aspectos esenciales para asegurar que la actividad de las Administraciones Públicas se encuentre sometida a Derecho teniendo en cuenta la singularidad que plantea el uso de medios electrónicos.

2. La limitada eficacia de las normas jurídicas en el contexto tecnológico de la Administración electrónica

En el actual estadio de evolución de la tecnología en el ámbito de las Administraciones Públicas existe una marcada tendencia a la multiplicación de los sistemas de recogida de información que, además, se han de interconectar como premisa elemental para la obtención de valor añadido (es el caso de las *ciudades inteligentes*), de manera que el origen de la información puede terminar difuminándose y, por tanto, la limitación de su uso para otros fines quedar irremediadamente dañada. Por otra parte, la generalización de los servicios basados en la computación en la nube nos aboca a potenciales conflictos de carácter internacional sobre la normativa aplicable y la jurisdicción competente, dificultando así de modo casi irremediable la efectiva tutela de los derechos y libertades, especialmente desde la perspectiva individual. Más aún, con la progresiva implantación de las conexiones en todo tipo de dispositivos y aparatos (*Internet de las Cosas*) las posibilidades de obtención

de información relativa a los hábitos y conductas de los usuarios se multiplican, y lo hacen más allá de los estrictos límites personales (caso de los teléfonos móviles, debido a su uso personal) para proyectarse incluso sobre los grupos y colectivos, como puede ser el caso de las familias. En fin, todo ello nos sitúa en un escenario tecnológico donde el *big data* encuentra un perfecto caldo de cultivo, en particular si tenemos en cuenta la propensión a difundir a través de las redes sociales todo tipo de información, documentos gráficos, opiniones o, simplemente, datos personales propios y de terceros.

Ante esta realidad, nuestra reflexión debe tener en cuenta una premisa indiscutible: la dificultad para el Derecho —por no hablar directamente de imposibilidad, al menos en algunos casos— de ofrecer respuestas adecuadas a la singularidad de los desafíos que plantea la tecnología, de manera que el control de calidad requerido para los servicios públicos se integre asimismo por un imprescindible elemento tecnológico (Jinesta, 2009: 25). Existe una tendencia, especialmente presente en culturas jurídicas continentales como la española, a que las normas jurídicas escritas predeterminen con suficiente precisión los supuestos de hecho a los que han de ser aplicadas, incurriendo con relativa frecuencia en un afán reglamentista que, por lo que ahora interesa, puede conllevar una importante limitación de su alcance. Ciertamente, la exhaustividad constituye una exigencia elemental en aquellos supuestos en que la regulación deba ser restrictiva, como sucede cuando conlleve una prohibición o se establezca una sanción, pero no con carácter general.

Se trata de un problema de especial trascendencia en el ámbito de la tecnología, donde el dinamismo constituye una de sus notas características, de manera que las normas podrían quedar desfasadas y, por tanto, no ser ya aplicables o, lo que incluso resulta más preocupante, aun siéndolo las consecuencias que se deriven llegaran a ser contrarias al objetivo inicialmente pretendido, tal y como puede suceder en aquellos casos en que las normas sobre protección de datos de carácter personal hayan sido aprobadas con anterioridad a la actual evolución de Internet y los servicios electrónicos actuales. Frente a esta realidad, los principios generales del Derecho adquieren una singular importancia a la hora de tratar de establecer mecanismos reguladores eficaces, si bien al mismo tiempo hay que admitir que una excesiva apertura en la determinación de su alcance puede generar un efecto

indeseable en forma de inseguridad jurídica. Así pues, por lo que se refiere a los derechos de los ciudadanos en el ámbito de la Administración electrónica, sería de gran importancia avanzar en la línea propuesta ya que, de lo contrario, reglas jurídicas excesivamente concretas —aunque, sin duda, bienintencionadas— pueden terminar convirtiéndose en el principal de los problemas a resolver.

Por otra parte, la destacada vinculación tecnológica de los tratamientos de información constituye un relevante desafío para el Derecho y, en concreto, para la eficacia de sus previsiones. En efecto, la seguridad jurídica y, en concreto, la aplicación de las disposiciones jurídicas descansa en gran medida en el efectivo respeto a las reglas técnicas que se establezcan, exigencia que ha de observarse al menos desde una doble consideración. Así, en primer lugar, las normas jurídicas deben establecer un nivel adecuado de protección desde la perspectiva de los estándares tecnológicos en función de la naturaleza de los riesgos existentes, concreción que no puede predeterminarse de manera absoluta a través de las fuentes del Derecho y, que por tanto, nos remite a la necesaria aplicación de criterios generalmente aceptados en el sector. Ahora bien, de nada sirve que la norma fije estándares muy garantistas —por ejemplo, normas de seguridad exigentes para la garantía de la privacidad de los ciudadanos, singularmente en relación a los denominados datos especialmente protegidos como los relativos a la salud— si en la práctica su incumplimiento no conlleva consecuencias jurídicas lo suficientemente contundentes como para desincentivar las conductas contrarias a las previsiones normativas. Y no se trata de establecer sanciones más o menos elevadas sino, sobre todo, de tratar de impedir —ya cautelarmente o, llegado el caso, de manera definitiva— la utilización de la información cuando no se hubiesen cumplido realmente las exigencias derivadas de la seguridad tecnológica.

En definitiva, el proceso de modernización tecnológica en que se encuentran inmersas las Administraciones Públicas conlleva una serie de relevantes desafíos desde la perspectiva jurídica (Martínez, 2009: 205 y ss.), entre los que cabe destacar a nuestros efectos el logro de un adecuado equilibrio entre las mayores posibilidades de eficacia que ofrece la tecnología y el pleno respeto a los derechos de los ciudadanos: se trata, en definitiva,

de establecer unas garantías equivalentes a las que configuran la posición jurídica del ciudadano cuando se relaciona con la Administración Pública de forma presencial utilizando el soporte papel (Gamero, 2010: 92). A este respecto, algunos textos constitucionales como el español han incorporado prevenciones frente al uso de la informática en relación con su incidencia en los derechos de los ciudadanos, si bien normalmente su alcance se ha vinculado al reconocimiento de un derecho a la protección de sus datos de carácter personal. Sin embargo, la vertiginosa innovación tecnológica que se está viviendo en los últimos años ha puesto de manifiesto la aparición de nuevos desafíos que van más allá de cualquier planteamiento reduccionista que se centre únicamente en el citado derecho. Más aún, existe un riesgo cierto de que una interpretación limitativa de las garantías jurídicas pueda llegar a producir una consecuencia indeseada, es decir, una disminución de la protección de los ciudadanos frente al uso de la informática y, por otra parte, mayores riesgos en cuanto a la efectividad de la tutela de los intereses públicos en juego.

Así pues, resulta imprescindible afrontar la problemática relación entre la seguridad jurídica y los aspectos tecnológicos desde una perspectiva más amplia que tenga en cuenta la singularidad de los servicios de Administración electrónica que se prestan en la actualidad, tanto por lo que se refiere al alcance de la posición jurídica de los ciudadanos como, asimismo, en relación al efectivo control por parte de los poderes públicos en la configuración y funcionamiento de las aplicaciones y los sistemas de información. Más aún, se trataría de superar la visión restrictiva que limite las consecuencias jurídicas del incumplimiento de las garantías tecnológicas al ámbito de la privacidad de los ciudadanos, ofreciendo vías adecuadas de protección a cualquier modalidad de uso de la informática que suponga una vulneración de sus derechos más allá de si la información vinculada a su persona física —identificada o, simplemente, identificable— se encuentra afectada sustancialmente. En última instancia, aun cuando las normas establezcan previsiones formales que, en apariencia, supongan una garantía para la posición jurídica de los ciudadanos, lo cierto es que con frecuencia su alcance está ciertamente limitado, pues en gran medida consisten en meras declaraciones genéricas sin efectiva trascendencia práctica.

3. El alcance jurídico de las normas técnicas: su efectivo respeto, una premisa inexcusable

El indiscutible protagonismo que corresponde a la tecnología en la modernización de los servicios públicos puede tener graves consecuencias para la seguridad jurídica y, por tanto, para la efectiva tutela de los derechos de los ciudadanos en sus relaciones con la Administración Pública. Dadas las dificultades para que normas jurídicas basadas en una concepción tradicional, esto es, pensadas para un contexto de documentos en papel y relaciones presenciales, desplieguen todos sus efectos cuando se proyectan sobre la realidad tecnológica, resulta imprescindible que, en última instancia, se asienten en un sólido fundamento tecnológico pues, de lo contrario, las garantías jurídicas podrían no desplegar su potencial como reglas dirigidas a la efectiva tutela de los intereses en juego. En última instancia, se trata de garantizar la superioridad de las normas jurídicas frente a los criterios, reglas y normas tecnológicas, de manera que no resulten socavados los cimientos del Estado de Derecho (Valero, 2013: 143).

Ahora bien, como se ha destacado certeramente (Esteve, 1999: 27), resulta ingenuo pretender un control absoluto de la tecnología por parte del Derecho, esto es, en relación a cada uno de los detalles y aspectos menores del funcionamiento de las aplicaciones informáticas y los sistemas de información. No por ello debe renunciarse al establecimiento, al menos, de una serie de requisitos mínimos y principios básicos a los que se ha de someter cualquier proyecto y servicio de Administración electrónica a fin de permitir la protección adecuada de la información. El riesgo consiste en que tales previsiones se limiten a meras recomendaciones y criterios programáticos cuya efectiva aplicación quede en manos de las respectivas Administraciones Públicas; antes bien, por el contrario, han de configurarse como auténticas normas jurídicas cuya infracción no puede quedar simplemente en el ámbito de las buenas prácticas —como sucede, por ejemplo, con los códigos de conducta— ya que, en última instancia, podría incluso afectar a la validez de las actuaciones que se lleven a cabo utilizando medios electrónicos.

La seguridad es uno de los pilares basilares a partir del cual se articula la Administración electrónica y, en este sentido, al margen de declaraciones implícitas resulta imprescindible que a nivel normativo se encuentre expre-

samente consagrada entre las finalidades y los principios que han de inspirar la implantación y utilización de medios electrónicos por las Administraciones Públicas. A este respecto, a fin de garantizar que su incumplimiento produzca consecuencias en cuanto a la invalidez de las actuaciones que se lleven a cabo vulnerando las reglas de seguridad, resulta imprescindible que estas últimas no se establezcan simplemente a través de meros actos administrativos sino, antes al contrario, se aprueben formalmente a través de normas jurídicas en sentido estricto, esto es, mediante una ley o, al menos, una disposición reglamentaria en la que se fijen los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

¿Cuáles son, por tanto, esos requisitos mínimos cuya vulneración podría afectar a las actuaciones y comunicaciones que lleven a cabo las Administraciones Públicas utilizando medios electrónicos o, en su caso, determinar la exigencia de responsabilidades, ya patrimonial a la institución ya personal a las autoridades y el personal al servicio de la correspondiente Administración Pública? Al margen de la efectiva implantación de, al menos unas medidas de seguridad generales en función de la naturaleza de la información a proteger y de la incidencia que puede tener la tecnología por lo que respecta a los usos previstos, también resulta de gran trascendencia que se establezcan ciertas obligaciones formales cuya inobservancia no supone necesariamente que no se hayan adoptado materialmente las precauciones correspondientes pero que, sin embargo, podrían ser un indicio de que no se satisfacen los estándares mínimos de seguridad (Valero, 2013: 182 a 186). ¿Cómo se ha de concretar, en el plano de la realidad, esta idea general?

- En primer lugar, debería ser obligatoria la aprobación formal de una política de seguridad en cada entidad, que tendrá que adaptarse de manera concreta a las características de la misma tanto por lo que se refiere a la perspectiva organizativa como, asimismo, a la naturaleza de la actividad que realice.
- En segundo lugar, para el análisis y el tratamiento de los riesgos de seguridad se ha de emplear una metodología reconocida internacionalmente a nivel de estándares, no bastando por tanto acudir a fórmulas que ofrezcan un menor nivel de garantía.
- Asimismo, con carácter previo a su instalación en el sistema, se debe requerir autorización expresa de cualquier elemento físico o

lógico a fin de constatar que cumple con las exigencias mínimas de seguridad.

- Finalmente, con la finalidad de asegurar el efectivo cumplimiento de las previsiones técnicas por lo que respecta a la seguridad, resulta preceptivo el registro de las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

El incumplimiento de tales medidas podría afectar a las garantías técnicas que han de respetar los servicios de Administración electrónica y, en consecuencia, a los derechos de los ciudadanos. Más allá de las consecuencias en orden a la responsabilidad patrimonial por los daños que se puedan haber causado —que exige una relación de causalidad que no siempre se dará—, la principal deficiencia de un eventual marco normativo en relación a la efectividad de las medidas exigidas por la seguridad desde la perspectiva tecnológica es la ausencia de consecuencias expresas en su articulado para hacer frente a los supuestos de incumplimiento, lo que sin duda conlleva un riesgo inadmisibles en cuanto a la seguridad jurídica.

Es por ello que, al menos en los supuestos más graves, en el caso de que, ya ocasionalmente o tras las oportunas auditorías periódicas que debieran establecerse con carácter preceptivo, habría que contemplar la posibilidad de que, al menos cautelarmente, se interrumpa la prestación del servicio durante el tiempo que estime prudente y, en todo caso, hasta la satisfacción de las modificaciones prescritas. Ahora bien, más allá de problemas ocasionales que pudieran producirse, la efectiva garantía del cumplimiento de las medidas de seguridad técnica adquiere una importancia singular que no debe menospreciarse en base a forzadas e inadmisibles justificaciones de afectación a los intereses públicos, de manera que en aquellos supuestos en que tenga lugar un claro y abierto menosprecio al cumplimiento de las medidas de seguridad debería bloquearse el funcionamiento de las aplicaciones, tal y como sucedería singularmente en el caso de que ni siquiera se lleven a cabo auditorías de seguridad conforme a las exigencias y el rigor que se hubiese establecido normativamente o, al menos, a través del acto por el que se apruebe el funcionamiento de las aplicaciones o los sistemas

de información que, siguiendo una de las iniciativas más destacadas en el ámbito europeo al respecto, denominaremos *acto base* siguiendo la terminología utilizada en el proyecto ReNEUAL, una de las iniciativas más relevantes en orden a la codificación del procedimiento administrativo (Mir y otros, 2015: 71 y ss.).

Aun cuando la tecnología puede ofrecer, en principio, mayores garantías que las actuaciones llevadas a cabo presencialmente —un ejemplo evidente es la posibilidad de suplantar la firma manuscrita o, sin ánimo exhaustivo, la incorporación de información adicional en los documentos electrónicos a través de los metadatos relativos a la modificación de los documentos—, lo cierto es que tal premisa requiere que se apliquen efectivamente las oportunas medidas de seguridad ya que, en caso de no hacerse, las consecuencias son ciertamente inevitables: se crea una apariencia formal de seguridad que en la práctica no se da y, por tanto, las posibilidades de accesos, alteraciones y manipulaciones indebidas se incrementan exponencialmente, afectando negativa e intensamente a la validez jurídica de aquellas, al margen, claro está, de otro tipo de consecuencias como la eventual responsabilidad que pueda derivarse o la desconfianza en la tecnología que puede generarse. Más aún, en muchos casos las propias Administraciones Públicas no adoptan las medidas técnicas necesarias para dar cumplimiento a las exigencias jurídicas, de manera que se implantan proyectos de modernización e innovación tecnológica en los que el grado de cumplimiento con las disposiciones normativas es más que deficiente.

Ante la constatación de esta evidencia surge la necesidad de plantear las consecuencias jurídicas que conlleva el incumplimiento de las garantías tecnológicas fijadas normativamente por lo que respecta a la Administración electrónica. Así, en primer lugar debe recordarse que la eventual garantía constitucional de la protección de los ciudadanos frente al uso indebido de la tecnología supone un refuerzo adicional que necesariamente ha de tener consecuencias por lo que respecta a la validez de las actuaciones administrativas que se lleven a cabo vulnerando su contenido. Más allá del plano constitucional, las consecuencias concretas por lo que respecta a la invalidez de las actuaciones administrativas deberían fijarse expresamente en relación a la singularidad que plantea la tecnología, si bien es cierto que habitualmente el legislador no suele especificarlas. En consecuencia,

se trata de una tarea que necesariamente habrá de llevarse a cabo por vía interpretativa, lo que puede suponer una dificultad adicional desde la perspectiva de la seguridad jurídica. En todo caso, debería entenderse que las actuaciones llevadas a cabo sin que se respeten las garantías esenciales de seguridad formalmente establecidas son inválidas, consecuencia que también se daría —al menos en nuestra opinión— en los supuestos de ausencia de un acto base en los términos antes indicados a pesar de las reticencias que se han mostrado por lo que respecta a la necesidad de aprobación formal de los programas y aplicaciones ante la inexistencia de consecuencias invalidantes (Suñé, 2000: 217). En dichos supuestos nos encontraríamos ante una vulneración sustancial de las garantías tecnológicas en las que se sustenta la seguridad jurídica, resultando de especial gravedad aquellos supuestos en que, como consecuencia de la infracción, se impida el pleno ejercicio de sus derechos a los ciudadanos, postura que no obstante no resulta pacífica a nivel doctrinal (Molina, 2010: 62).

Esta misma consecuencia se daría en el supuesto en que la infracción conlleve la vulneración manifiesta de las reglas de competencia por razón de la materia, problemática en relación con la cual las actuaciones automatizadas ofrecen una especial trascendencia. En efecto, podría darse el caso de que las reglas competenciales hayan reservado a un determinado órgano administrativo una concreta actuación, de manera que mientras permanezcan vigentes se requerirá necesariamente al menos la intervención del mismo a través del correspondiente sello de órgano; de manera que no serviría otro instrumento para asegurar la integridad y autenticidad de la misma. Más aún, también habrían de respetarse las exigencias esenciales que, desde el punto de vista sustantivo, se hayan fijado para las actuaciones automatizadas, en particular las que se refieren a las condiciones técnicas para su correcto funcionamiento. Sería el caso, por ejemplo, de la ausencia de los informes preceptivos sobre las aplicaciones o, sin ánimo exhaustivo, el incumplimiento de reglas jurídicas adaptadas a la singularidad de la tecnología como la privacidad por diseño.

Además de tales requisitos, con carácter general es necesario que el incumplimiento de las medidas de seguridad y la causa de invalidez tengan una relación directa que justifique el alcance de tales consecuencias, no bastando por tanto la simple concurrencia de circunstancias genéricas y abstractas como

el mero hecho de no haber implantado las medidas de seguridad previstas en cada caso según el tipo de servicio o el trámite de que se trate. En estos casos, por el contrario, aunque no pueda afirmarse la invalidez de la actuación realizada, sí que se deberían adoptar de oficio —y, por supuesto, a solicitud del interesado— la medida cautelar que consiste en la paralización del funcionamiento de los servicios afectados hasta que no se satisfagan las garantías técnicas previstas en la normativa que, en cada caso, resulte de aplicación.

4. El necesario refuerzo de los intereses públicos y de los derechos de los ciudadanos

El acceso a la información y su difusión a través de medios electrónicos constituye una exigencia inexcusable en el actual estado de evolución tecnológica de la sociedad, tanto por razones de eficiencia como de fortalecimiento del carácter democrático de las Administraciones Públicas. Sin embargo, con frecuencia la regulación de este derecho se plantea como una mera adaptación al soporte electrónico de un modelo de gestión tradicional, es decir, a partir del acceso a documentos en un sentido estricto, aun cuando se pretendan utilizar medios telemáticos. En consecuencia, se asume un planteamiento ciertamente limitado que desconoce las posibilidades que ofrece la tecnología al permitir reconfigurar el alcance del objeto del derecho de acceso de los ciudadanos más allá del mero conocimiento de los documentos (Muñoz y Bermejo, 2014: 207 a 224); perspectiva innovadora que ha de ser asimismo asumida como una posibilidad de reforzar la posición jurídica de los ciudadanos en relación con el uso de medios tecnológicos por parte de las entidades públicas, ofreciendo una manifestación avanzada del llamado Gobierno Abierto desde la perspectiva tecnológica (Martín, 2014: 404).

Por otra parte, la tutela de la posición jurídica de los ciudadanos debe convertirse en uno de los ejes principales en los que sustentar la innovación tecnológica en el ámbito que nos ocupa, en particular por lo que se refiere al tratamiento de sus datos personales. Teniendo en cuenta la tendencia a fragmentar la unidad de gestión informativa y, de esta manera, desplazar el protagonismo desde los documentos a los datos (Valero, 2013: 293 a 299), resulta imprescindible asegurar la efectiva aplicación de las limitaciones en cuanto a su utilización, para lo cual los metadatos y cualesquiera otros elementos que permitan contextualizar su origen están llamados a jugar un destacado

papel; lo que, por tanto, nos remite a la necesidad de reforzar los estándares de gestión documental desde esta perspectiva. Más aún, en la medida que los intercambios de información están llamados a intensificarse, no puede obviarse que conceptos como la interoperabilidad deben contemplarse necesariamente no sólo desde la perspectiva técnica y organizativa sino que, por lo que respecta a nuestro enfoque, habrán de reforzarse desde el prisma jurídico. En efecto, como se ha explicado (Gamero, 2009: 292 y ss., Cerrillo, 2010: 757 y ss.), este principio constituye la piedra angular para el impulso de la Administración electrónica integral, de manera que su dimensión jurídica adquiere una importancia singular. En consecuencia, los niveles de protección que ofrece el Derecho se tienen que proyectar en el diseño de las aplicaciones y el funcionamiento de los sistemas de información, planteamiento que resulta de especial relevancia por lo que se refiere a las demandas de accesibilidad y transparencia informativa que se plantean a las Administraciones Públicas, tensión a la que sólo puede hacerse frente desde los planteamientos de la privacidad por el diseño (Martínez, 2014: 277 a 280, Valero, 2013: 392 a 394). Nos encontramos con una exigencia de singular trascendencia en un contexto de gestión basado en el incremento sustancial de las interconexiones, por una parte, y, por otro, de las comprobaciones y actuaciones automatizadas a que abocan las medidas de simplificación emprendidas en los últimos años, tanto por lo que se refiere a la efectividad del derecho a no presentar documentos que ya obren en poder de las Administraciones Públicas como, asimismo, a la implantación de modelos liberalizadores articulados a partir de comunicaciones previas y declaraciones responsables, lo que obliga a un rediseño de los mecanismos de control que necesariamente han de configurarse *a posteriori*, esto es, una vez iniciada la actividad privada a supervisar. Se trata, en última instancia, de hacer frente a las implicaciones jurídicas que conlleva la gobernanza de la interoperabilidad, especialmente trascendentes en contextos supranacionales como la Unión Europea o Latinoamérica, que habrán de tener en cuenta necesariamente aspectos tan cruciales como los estándares de seguridad mínimos en los intercambios digitales que, entre otros aspectos, deben considerar la existencia de unas pautas legales comunes que no los impidan (Criado, 2009: 30).

Más aún, la utilización de medios electrónicos por parte de las Administraciones Públicas implica con frecuencia la realización de actuaciones

automatizadas, lo que sin duda conlleva importantes implicaciones desde la perspectiva jurídica. Así, resulta imprescindible que la Administración conserve su capacidad de decisión en aspectos tan relevantes como la definición de las especificaciones, programación, mantenimiento, supervisión, control y, en su caso, auditoría del sistema de información y del código fuente de las aplicaciones, debiendo concretarse en última instancia quién se considera responsable de la actuación de que se trate a los efectos de impugnaciones y, adicionalmente, a quién corresponde formalmente adoptar las decisiones materiales relativas a dichos aspectos y, en su caso, realizar los informes técnicos procedentes. En última instancia, se trataría de asegurar que se cumplan las exigencias generales de respeto del ejercicio competencial por parte del órgano que, según la actividad de que se trate, deba tomar la decisión y, desde la perspectiva de la identificación y autenticación, con las previsiones específicas que en cuanto al uso de firma electrónica resulten exigibles para las actuaciones automatizadas.

Desde esta premisa adquiere singular importancia que las aplicaciones informáticas y los sistemas de información que se utilicen sean aprobados formalmente por la entidad pública donde vayan a ser utilizados —por ejemplo, a través de un acto administrativo, no siendo imprescindible una norma reglamentaria—, especialmente en aquellos supuestos es que su funcionamiento pueda afectar a los derechos y libertades de los ciudadanos. Pero, por lo que respecta a la proyección de las exigencias de transparencia y accesibilidad de la información, es necesario establecer una exigencia normativa clara en orden a la difusión pública de sus características, en particular vinculando su incumplimiento a la concurrencia de consecuencias sobre la invalidez de la actuación administrativa que tuviera lugar al margen de la misma (Palomar, 2005: 22), en particular mediante la utilización del diario oficial que corresponda. De esta manera se habilitaría la posibilidad de realizar una impugnación autónoma del acto de aprobación formal de las aplicaciones y los sistemas de información que, por lo que ahora interesa, permitiría discutir la adecuación de las medidas de seguridad que se contemplen en dicho acto que, por razones obvias, está llamado a desplegar efectos generales sobre todas aquellas decisiones y actuaciones que se realicen a su amparo que, por su parte, también podrían ser impugnadas individualmente en la medida que no se ajusten a las previsiones de aquél (Palomar, 2005: 84 a 87).

No obstante, debemos manifestar nuestra discrepancia con algunos de los argumentos del citado autor ya que, una vez sentada dicha consecuencia invalidante y tras afirmar que “debería inhabilitar a la Administración para su utilización (en el plano interno)”, extrae una consecuencia distinta e incluso incompatible *ad extra*, ya que admite que se pueda demostrar que, a pesar de la falta de aprobación, su utilización no ha mermado ni perjudicado la decisión adoptada, “que se ha confeccionado conforme a Derecho” (*ibídem*: 87). Incluso, más adelante el citado autor llega a considerar que la aprobación de la aplicación tiene carácter normativo, de manera que en su opinión cabría interponer un recurso indirecto en sede judicial (*ibídem*: 88 y 89).

La garantía relativa a la transparencia y el acceso a la información debería ser completada con el reconocimiento expreso —o, en su caso, implícitamente derivado de la garantía constitucional que se establezca para la defensa de los derechos e intereses legítimos— de un derecho por parte de los ciudadanos a obtener toda aquella información que permita la identificación de los medios y aplicaciones utilizadas, así como del órgano bajo cuyo control permanezca el funcionamiento de la aplicación o el sistema de información. Este derecho podría ejercerse en los supuestos en que la publicidad del acto base no se hubiere impuesto normativamente, debiendo admitirse la posibilidad de atacar por medios directos e indirectos la aprobación de las aplicaciones y sistemas informáticos al considerarla una norma jurídica (Fernando, 1993: 114 y 115). Incluso, el objeto de este derecho debería incluir no sólo el conocimiento del resultado de la aplicación o del sistema informativo que le afecte específicamente a su círculo de intereses sino, además y sobre todo, debería extenderse al origen de los datos empleados y la naturaleza y el alcance del tratamiento realizado, es decir, a cómo el funcionamiento de aquellos puede dar lugar a un determinado resultado. En todo caso, la configuración de este derecho habría de permitir conocer tales extremos no sólo cuando se refieran a la decisión que se adopte sino que, asimismo, debería proyectarse sobre los actos de trámite, tal y como sucede singularmente con los informes, borradores y documentación complementaria.

Se trata, en definitiva, de ofrecer una mínima transparencia en el funcionamiento de los instrumentos técnicos utilizados para el desarrollo de la actividad administrativa a través de medios electrónicos: a diferencia de lo que sucede en las actuaciones tramitadas en soporte papel y basadas exclu-

sivamente en la decisión adoptada por el titular del órgano administrativo, la mediación de un programa o aplicación informática implica una interferencia en el proceso normal de producción de la actividad administrativa, ya que un resulta un instrumento esencial para que el ciudadano conozca el proceso de formación de la decisión administrativa (Palomar, 2005: 380). En efecto, como se ha destacado con acierto, la aplicación de las tecnologías de la información y la comunicación en las decisiones adoptadas por las Administraciones Públicas conlleva un radical cambio de los parámetros en que tradicionalmente se han sustentado, de manera que la respuesta de la persona física responsable de la misma —ya sea el titular del órgano competente, ya un funcionario de *a pie*— viene condicionada en gran medida por la programación que previamente se haya realizado de la aplicación en cuestión (Bovens y Zouridis, 2002: 177 y ss.). De ahí que no podamos compartir planteamientos reduccionistas tendentes a minimizar el alcance de las previsiones que puedan existir a tales efectos, en particular si se esgrime la naturaleza meramente interna de los actos de aprobación (González y Alenza, 2002: 471) puesto que, en definitiva, van a afectar directa y sustancialmente a los derechos e intereses de los ciudadanos. En efecto, sólo partiendo de estos presupuestos se comprende el sentido último de la obligación analizada, esto es, que el ciudadano conozca los programas y aplicaciones que van a ser utilizados para realizar una actuación administrativa que le afecta, de manera que disponga de los elementos de juicio necesarios para defenderse frente a eventuales irregularidades de la actuación administrativa motivadas por la vulneración de las garantías tecnológicas que han de respetar las aplicaciones y los sistemas de información.

5. La garantía del efectivo cumplimiento de las garantías tecnológicas

Al margen del establecimiento de exigencias normativas en orden a la adopción de las medidas de seguridad de carácter tecnológico al que nos hemos referido anteriormente, de nada sirve con su mera previsión si las consecuencias jurídicas del incumplimiento no se encuentran aseguradas suficientemente. Además de las implicaciones referidas a la invalidez de las actuaciones ya examinada y que, en última instancia, habrán de ser apreciadas por parte de los órganos judiciales, la creación de órganos o entidades

específicamente dedicados a exigir su cumplimiento constituye una medida elemental. A este respecto, cabe plantear diversas soluciones que, al margen de su mayor o menor garantía desde el punto de vista institucional, han de ser adoptadas teniendo en cuenta circunstancias que no siempre se apoyan en estrictos criterios de lógica jurídica sino, más bien, de naturaleza política.

Dejando a un lado estas últimas consideraciones, podrían plantearse varios escenarios (Valero y Pardo, 2012). Así, en primer lugar que el control del cumplimiento corresponda a una entidad dotada de autonomía institucional, de manera que sus decisiones no estuvieran condicionadas por la dependencia de las autoridades u organismos a controlar. Ciertamente, esta opción no siempre será viable desde la perspectiva presupuestaria, por lo que alternativamente se podría encomendar las funciones a los organismos encargados de tutelar el derecho a la protección de los datos personales de los ciudadanos y/o, en su caso, el cumplimiento del marco normativo sobre transparencia y acceso a la información administrativa; entidades que suelen estar dotadas de un estatuto jurídico de independencia que las haría especialmente idóneas para llevar a cabo las tareas de control y supervisión del efectivo respeto a las exigencias tecnológicas de los servicios y aplicaciones. Ahora bien, en el caso de que dichas iniciativas fuesen descartadas, debería al menos asignarse la función a un órgano interno propio de la correspondiente entidad, aunque en este caso sería de especial importancia que tuviese garantizado un estatuto de autonomía funcional, de manera que no estuviera sometido a órdenes ni instrucciones y, por otra parte, no se integrase en la estructura jerárquica de la entidad. Se trataría, por tanto, de asegurar que sus decisiones fueran realmente objetivas y, en última instancia, que sus informes y decisiones obedecieran únicamente al estricto respecto de las previsiones relativas a la seguridad de las aplicaciones y sistemas de información desde la perspectiva técnica y, por tanto, jurídica.

Sin embargo, la garantía de independencia o autonomía funcional resulta insuficiente si dicha entidad u órgano no está dotada de instrumentos adecuados para cumplir la finalidad prevista: en última instancia, que se respeten las medidas de seguridad que contemplan las normas o, en su caso, las actuaciones no normativas formalmente adoptadas en los términos antes referidos. Por esta razón, se les debe atribuir la potestad de inmovilización de las aplicaciones y los sistemas de información en aquellos supuestos

de incumplimiento más grave de las reglas de seguridad, especialmente si pueden verse afectados los derechos y libertades de los ciudadanos o la correcta adopción de las decisiones administrativas. Ciertamente, aun cuando siempre podría acudir a otros mecanismos de carácter general como la responsabilidad patrimonial por los daños que eventualmente se puedan causar o, según se analizó anteriormente, la invalidez de las actuaciones administrativas, lo cierto es que se trata de consecuencias que sólo tienen lugar a *posteriori* y, al menos en el caso de la responsabilidad patrimonial, que únicamente podrían convertirse en un incentivo adecuado en el supuesto de que los daños fuesen elevados en su cuantía, ya por su propia naturaleza ya por la existencia de un elevado número de personas afectadas. Sin embargo, teniendo en cuenta la singularidad del ámbito analizado, lo cierto es que difícilmente podrían darse dichas condiciones, de manera que las referidas consecuencias habrían de considerarse al menos un estímulo indirecto para el efectivo respeto de las medidas de seguridad.

6. Consideraciones finales

La modernización tecnológica de las Administraciones Públicas está llamada a incrementar la complejidad de las relaciones jurídicas, de manera que resulta imprescindible una mayor transparencia en el funcionamiento de las aplicaciones y los sistemas de información. En este sentido, la exigencia se ha de referir no sólo a la perspectiva estrictamente jurídica del acceso a la información sino, además y sobre todo, a los aspectos técnicos, de modo que no termine por consolidarse una suerte de opacidad que impida el efectivo control de los poderes públicos.

Esta necesidad adquiere una especial importancia si analizamos los proyectos que se están impulsando en los últimos tiempos y que, sin duda, se van a reforzar en un futuro más inmediato, tal y como sucede con las ciudades inteligentes, el *big data* o la colaboración público-privada en la creación de nuevos e innovadores servicios basados en el uso intensivo de información en manos de los poderes públicos. De lo contrario existe un riesgo cierto de crear una burocracia electrónica inmune al efectivo control por parte de la ciudadanía que, en última instancia, podría afectar seriamente a la calidad democrática de la actividad que llevan a cabo dadas las dificultades de someterla a la primacía de las normas jurídicas. Está en juego, por tanto,

la efectividad del Estado de Derecho en el contexto de la innovación tecnológica a la que están abocadas las Administraciones Públicas.

7. Ideas y conceptos principales

- **Actuación administrativa automatizada:** Actuación administrativa producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular. Incluye la producción de actos de trámite o resolutorios de procedimientos, así como de meros actos de comunicación.
- **Documento administrativo electrónico:** aquel documento administrativo que ha sido generado por medios informáticos o se conserva en dicho soporte. Se entiende por documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado. Siempre que respeten las oportunas medidas de seguridad, tienen el mismo valor y eficacia que los generados o almacenados en papel siempre que se garantice su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado. En este sentido han de incorporar una o varias firmas electrónicas.
- **Estándar abierto:** aquel que sea público y su utilización sea disponible de manera gratuita o a un coste que no suponga una dificultad de acceso, además de que su uso y aplicación no esté condicionado al pago de un derecho de propiedad intelectual o industrial.
- **Interoperabilidad:** capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.
- **Neutralidad tecnológica:** principio en virtud del cual la Administración Pública no puede decantarse por un determinado sistema operativo o por una concreta aplicación a la hora de desarrollar sus sistemas de información y, por extensión, a la hora de relacionarse con los ciudadanos.

Preguntas de repaso

1. ¿Qué papel piensa que debe jugar el Derecho en la regulación de los aspectos tecnológicos de la Administración electrónica?
2. Desde una perspectiva jurídica, ¿cuáles considera que han de ser las exigencias mínimas de naturaleza tecnológica que han de respetarse a la hora de poner en marcha un proyecto relacionado con el uso de medios electrónicos por parte de las Administraciones Públicas?
3. En relación con la regulación de la Administración electrónica en su respectivo país, ¿considera suficiente la regulación jurídica relativa a los riesgos específicos que plantea la tecnología?
4. ¿Hasta qué punto le parece adecuada la regulación relativa al soporte electrónico de los documentos administrativos? ¿Piensa que está garantizada la integridad y autenticidad de la información en poder de la Administración Pública con independencia de que se encuentre en soporte papel o electrónico? ¿Cuál de dichos soportes le parece más seguro?
5. ¿Considera que la mayor incidencia que supone el uso de la tecnología para los derechos de los ciudadanos debe tener una regulación más estricta? En concreto, ¿qué medidas adoptaría por lo que se refiere a la privacidad?
6. Los proyectos relacionados con la innovación tecnológica —ciudades inteligentes, redes sociales *big data*, servicios en la nube...— suponen un gran avance desde la perspectiva de la eficacia, la eficiencia y la personalización de los servicios, pero ¿considera que las garantías jurídicas actuales son adecuadas y suficientes para este contexto? En concreto, ¿qué medidas cree que debieran adoptarse?

Referencias

- Alamillo Domingo, Ignacio** (2012). «Seguridad y firma electrónica: marco jurídico general», en E. Gamero y J. Valero (coords), *Las Tecnologías de la Información y la Comunicación en la Administración de Justicia*. Thomson-Aranzadi, Cizur Menor.
- Alamillo Domingo, Ignacio y Uríos Aparisi, Xavier** (2011). *La actuación administrativa automatizada en el ámbito de las Administraciones Públicas*, Escuela de Administración Pública de Cataluña.
- Boix Palop, Andrés** (2007). «La neutralidad tecnológica como exigencia regulatoria en el acceso electrónico a los servicios administrativos». *Revista General de Derecho Administrativo*, núm. 16.
- Bovens, Mark Y Zouridis, Stavros** (2002). «From Street-Level to System-Level Bureaucracies: How Information and Communication Technology is Transforming Administrative Discretion and Constitutional Control». *Public Administration Review*, vol. 62, núm. 2.
- Cerrillo i Martínez, Agustí** (2010). «Cooperación entre Administraciones Públicas para el impulso de la Administración electrónica». En E. Gamero y J. Valero (coords.), *La Ley de Administración electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos*, 3ª ed. Cizur Menor: Thomson Reuters-Aranzadi.
- Criado Grande, Juan Ignacio** (2009). «Gobierno electrónico en Latinoamérica. Aproximación desde una perspectiva intergubernamental». *Revista chilena de Administración Pública*, núm. 14.
- Esteve Pardo, José** (1999). *Técnica, riesgo y Derecho*. Ariel.
- Fernando pablo, Marcos Matías** (1993). «Administración Pública, informática y ciudadanos: perspectiva general». *Informática y Derecho*, núm. 2.
- Gamero Casado, Eduardo** (2009). «Interoperabilidad y Administración electrónica: conéctense, por favor». *Revista de Administración Pública*, núm. 179.
- Gamero Casado, Eduardo** (2010). «Objeto, ámbito de aplicación y principios generales de la Ley de Administración electrónica: su posición en el sistema de fuentes». En E. Gamero y J. Valero (coords.), *La Ley de Administración electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de*

- Acceso Electrónico de los Ciudadanos a los Servicios Públicos*. Cizur Menor: Thomson Reuters-Aranzadi.
- González Navarro, Francisco y Alenza García, José Francisco** (2002). *El derecho de petición*. Madrid: Civitas.
- Jinesta, Ernesto** (2009). «Administraciones Públicas Electrónicas: Retos y Desafíos para su regulación en Iberoamérica». *Desafíos del Derecho Administrativo Contemporáneo*. Universidad Andrés Bello, Venezuela.
- Martín Delgado, Isaac** (2014). «Transparencia, reutilización y datos abiertos». En J. Valero y M. Fernández (coords.), *Régimen jurídico de la transparencia del sector público. Del derecho de acceso a la reutilización de la información*. Cizur Menor: Thomson Reuters-Aranzadi.
- Martín Delgado, Isaac** (2009). Naturaleza, concepto y régimen jurídico de la actuación administrativa automatizada». *Revista de Administración Pública*, núm. 180.
- Martínez Gutiérrez, Rubén** (2009). *Administración Pública electrónica*. Cizur Menor: Thomson Reuters-Civitas.
- Martínez Martínez, Ricard** (2014). «De la opacidad a la casa de cristal. El conflicto entre privacidad y transparencia». En J. Valero y M. Fernández, *Régimen jurídico de la transparencia del sector público. Del derecho de acceso a la reutilización de la información*. Cizur Menor: Thomson Reuters-Aranzadi.
- Mir Puigpelat, Oriol y otros, editores** (2015). *Código ReNEUAL de procedimiento administrativo de la Unión Europea*. Versión inglesa accesible a través de Internet en <http://www.reneual.eu/> (última visita: 28/01/2015).
- Muñoz Soro, José Félix y Bermejo Latre, José Luis** (2014). «La redefinición del ámbito objetivo de la transparencia y el derecho de acceso a la información del sector público». En J. Valero y M. Fernández (coords.), *Régimen jurídico de la transparencia del sector público. Del derecho de acceso a la reutilización de la información*. Cizur Menor: Thomson Reuters-Aranzadi.
- Molina Mateos, José María** (2010). «Esquema Nacional de Seguridad». *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 23.
- Palomar Olmeda, Alberto** (2005). «El acto administrativo dictado sobre bases tecnológicas o informáticas y las pautas de su revisión jurisdiccional». *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 7.

Palomar Olmeda, Alberto (2007). *La actividad administrativa efectuada por medios electrónicos*. Thomson-Aranzadi, Cizur Menor

Piñar Mañas, José Luis (2011). «Revolución tecnológica y nueva Administración», en J.L. PIÑAR (dir.), *Administración electrónica y ciudadanos*. Thomson-Civitas, Cizur Menor.

Suñé Lliñás, Emilio (2000). «El procedimiento administrativo en la era digital: la necesidad de entidades de certificación». En Luis Jordana de Pozas. *Creador de Ciencia Administrativa*. Madrid: Servicio de Publicaciones de la Facultad de Derecho de la Universidad Complutense.

Valero Torrijos, Julián (2013). *Derecho, innovación y Administración electrónica*. Sevilla: Global Law Press.

Valero Torrijos, Julián y Pardo López, María Magnolia (2012). «Institutional Backing and PSI Reuse: Is the EU Going Too Far or Just Going in the Wrong Way?». *Masaryk University Journal of Law and Technology (MUJLT)*, vol. 6(3).

Otras lecturas

Cotino Hueso, Lorenzo y Valero Torrijos, coords. (2010), *La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y los retos jurídicos del e-gobierno en España*. Tirant: Valencia.

Gamero Casado, y J. Valero Torrijos, coords. (2010), *La Ley de Administración electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos*, 3ª ed. Thomson-Aranzadi: Madrid.

Piñar Mañas, José Luis (2011). «Revolución tecnológica y nueva Administración», en J.L. Piñar (dir.), *Administración electrónica y ciudadanos*. Thomson-Civitas, Cizur Menor.

Rodríguez Adrados, Antonio (2015). «La firma electrónica y su utilización por un tercero». En Francisco Javier García Mas, *El documento electrónico. Un reto a la seguridad jurídica*. Dykinson: Madrid.

Valero Torrijos, Julián (2007). *El régimen jurídico de la e-Administración. El uso de medios informáticos y telemáticos en el procedimiento administrativo común*, 2ª ed. Comares, Granada.



Julián Valero es Profesor Titular (acreditado como Catedrático) de Derecho Administrativo en la Universidad de Murcia e investigador responsable del grupo *Innovación, Tecnología y Derecho* (iDerTec). Premio Nacional de Investigación *Marcelo Martínez Alcubilla* otorgado por el Instituto Nacional de Administración Pública. Participa en diversos proyectos de investigación relacionados con las referidas temáticas. Es autor y coordinador de numerosas publicaciones en el ámbito del uso de medios electrónicos en la actividad del sector público, en particular por lo que respecta a la e-Administración, la protección de los datos de carácter personal y el acceso y la reutilización de la información del sector público y el *open data*. En particular destaca la monografía *Derecho, innovación y Administración electrónica*, publicada en 2013 por la editorial Global Law Press. Asimismo, es coordinador académico de las jornadas SICARM/Congreso Derecho TICs, que se vienen organizando en la Universidad de Murcia desde hace diez años y que se dedican al análisis de las implicaciones jurídicas de la innovación tecnológica, especialmente por lo que respecta a las Administraciones Públicas. Las intervenciones correspondientes a dicha actividad se encuentran disponibles a través de Internet en www.sicarm.es

Para citar el presente capítulo: Valero, Julián (2016) “Seguridad, tecnología y Administración Pública electrónica: La necesaria reconfiguración del alcance de las garantías jurídicas ante la innovación tecnológica”, en J. R. Gil-García, J. I. Criado y J. C. Téllez (eds). *Tecnologías de Información y Comunicación en la Administración Pública: Conceptos, Enfoques, Aplicaciones y Resultados*, México, INFOTEC, pp. 135-160.

