Esta tesis doctoral afronta el estudio jurídico del proceso de desarrollo del *software* de las Administraciones públicas desde la óptica de la seguridad de nuestra naciente Administración electrónica, un tema escasamente tratado en la literatura especializada.

Los capítulos iniciales centran los conocimientos básicos en los que se apoya este trabajo desde un triple enfoque, que incluye un acercamiento somero a los elementos tecnológicos involucrados (evitando en lo posible términos técnicos), un viaje cronológico a lo largo del camino que ha recorrido el Derecho hasta culminar en el actual marco jurídico europeo y nacional, y unas pinceladas sobre los aspectos operativos que pueden dificultar la implantación con éxito de la Administración electrónica.

Las distintas dimensiones de la seguridad (autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad) pueden verse afectadas por el modo en que se desarrolle el *software* de nuestras Administraciones públicas, unos programas que contienen errores con elevada frecuencia, defectos ocultos que ocasionan tasas elevadas de fallos al inicio de la vida de un programa y que se disparan con incrementos bruscos tras introducir cambios en el código.

Sobre los desarrolladores descansa una gran responsabilidad. Una programación inadecuada puede llevar incluso al repudio de la firma digital por el ciudadano inocente, sumiéndolo en una difícil situación legal que le obliga a proporcionar una prueba cercana a lo imposible. Recae también sobre ellos el respeto al principio de neutralidad tecnológica, difícil de alcanzar ante la gran diversidad de tecnologías actuales

y con perniciosos efectos sobre los obligados a relacionarse con la Administración electrónicamente, a quienes, además, se les niega el derecho a recibir asistencia, sin que los Tribunales sean proclives a apreciar este hecho, cargando a la ciudadanía las consecuencias de la incapacidad de nuestras Administraciones públicas para seguir el ritmo de la tecnología.

Con la ley de acceso electrónico de los ciudadanos a los servicios públicos se dio el paso del "podrán" al "deberán", reconociendo el derecho y la obligación correlativa de la Administración. Su abanderado, el derecho del ciudadano a no aportar datos y documentos que ya obren en poder de las Administraciones públicas, apunta hacia un modelo de Administración electrónica de intercambiabilidad total de datos, con consentimiento del interesado. Materializado por una "plataforma de intermediación de datos" cuyos primeros pasos surgieron para sustituir la aportación de fotocopias de documentos de identidad por una consulta al sistema, ha evolucionado de forma continuada, añadiendo nuevos cedentes de información. Esa interconexión de bases de datos públicas, premiada internacionalmente, crece día a día, por la comodidad que proporciona al ciudadano y la celeridad que permite a la Administración.

En esta tesis doctoral se analiza el peligro que supone esa plataforma para el derecho fundamental a la protección de los datos de carácter personal y se propone una sencilla solución técnica que permitiría su uso controlado por el ciudadano, de una forma coherente con el nuevo Reglamento general de protección de datos europeo, orientado al análisis y prevención de los riesgos.

El artículo 28 de la nueva ley 39/2015 mantiene el modelo de intercambiabilidad total, presentando una redacción algo confusa que, además, ha incorporado una modificación del texto del anteproyecto pedida por la Agencia española de protección de datos, pero la ha insertado en un lugar equivocado del artículo. Esta recién estrenada ley está llamada a ser modificada, no solo por esta desafortunada redacción, sino para eliminar la presunción de consentimiento salvo oposición expresa, rechazada por el nuevo Reglamento europeo.

La también nueva ley 40/2015, de régimen jurídico del sector público, modifica la definición de "actuación administrativa automatizada", eliminando la exigencia de que esté adecuadamente programada, pasando así a admitir que el *software* de las Administraciones públicas puede ser defectuoso. Confrontando el contenido de su artículo 41.2 con los pasos definidos por la metodología para el desarrollo del *software* Métrica V3, creada por y para las Administraciones públicas, esta tesis doctoral se pronuncia sobre cuáles son las tareas susceptibles de externalización y qué trabajos deben descansar necesariamente sobre los hombros de los empleados públicos adscritos a cuerpos especializados.

Pero la Administración ha confiado a sujetos privados la realización de determinadas funciones, lo que supone la sustitución del empleado público por el trabajador externo, bajo la creencia generalizada de que el coste de esta alternativa es menor y constituye un factor de eficacia y eficiencia, empujada también por la prohibición de incorporar nuevo personal fijo, sufrida durante los últimos años, que ha empobrecido

las plantillas de muchos servicios públicos, conduciendo a la pérdida de control y de conocimiento asociada a la dependencia de empresas privadas.

Las recientes instrucciones recibidas por los empleados públicos en aras a evitar las demandas por cesión ilegal de trabajadores, dificultan aún más la obtención de un *software* de calidad mediante la externalización.

En los contratos de servicios de carácter intelectual, como el de desarrollo de aplicaciones a medida, se requiere una cualificación importante del personal del contratista que, en unión con la práctica imposibilidad de que un informático que no ha realizado materialmente las tareas de programación pueda validar su corrección en un tiempo razonable, empuja a la Administración hacia un preocupante comportamiento orientado a celebrar el contrato con alguien a quien ya conoce y que le inspira confianza.

Llegado ya ese *software* a un entorno de riesgo como es el de producción, debemos recordar que la tramitación telemática no equivale a procedimiento anónimo e irresponsable. Habida cuenta de que la responsabilidad es una garantía para el ciudadano, cuando el fallo informático cause un daño indemnizable, podrá ser objeto de responsabilidad patrimonial. Recae sobre nuestras Administraciones públicas el deber de garantizar unos servicios eficientes y de calidad, manteniendo el control en el caso de externalización, de forma que puedan garantizar los derechos de los ciudadanos, algo que difícilmente podrán lograr si no mantienen un dominio y control reales.

Examinadas diversas decisiones jurisprudenciales relacionadas con la Administración electrónica, se observa que las alegaciones referentes al mal

funcionamiento de las aplicaciones públicas por parte de los ciudadanos o de las empresas obligadas a utilizar los medios electrónicos, frecuentemente fracasan por la dificultad de cumplir con la carga de la prueba. Los Tribunales consideran la actitud diligente como criterio para inclinar la balanza de la justicia, pero normalmente no analizan la vulneración del principio de neutralidad tecnológica, ni se adentran a examinar el incumplimiento de la obligación de implantar las medidas de seguridad establecidas por el Esquema Nacional de Seguridad.

Sabedores de que el *software* no siempre funcionará adecuadamente, sobre los desarrolladores recae el peso de la seguridad, imprescindible para la tutela de los derechos y el normal funcionamiento de la actividad administrativa. Los principios básicos y requisitos mínimos establecidos en nuestro ordenamiento jurídico para mantener un entorno controlado, equilibrando seguridad y productividad desde el diseño y por defecto, adolecen de consecuencias expresas a su incumplimiento, con el riesgo de que se relaje el riguroso cumplimiento de la normativa.