LA CIBERSEGURIDAD PÚBLICA: UN RETO PERMANENTE

por

Prof. Dr. Carlos Galán Pascual

Profesor de la Universidad Carlos III de Madrid y Presidente de la Agencia de Tecnología Legal

Doctor en Informática y Abogado especialista en Derecho de las TIC

Y

Carlos Galán Cordero

Abogado y Consultor Jurídico-Tecnológico de la Agencia de Tecnología Legal

1. INTRODUCCIÓN: LA SEGURIDAD COMO CONCEPTO POLIÉDRICO.

El **VI Congreso Nacional de Innovación y Servicios Públicos (CNIS 2016)**, entre los temas que han conformado su extenso programa, ha contemplado también **la seguridad en la prestación de los servicios públicos.**

Como es sabido, la seguridad de los servicios públicos –no sólo la de aquellos que comprenden el desarrollo del procedimiento administrativo- es un concepto poliédrico que involucra muchos aspectos y que puede y debe abordarse en la actualidad desde distintas perspectivas, que se esquematizan sumariamente en la figura siguiente.

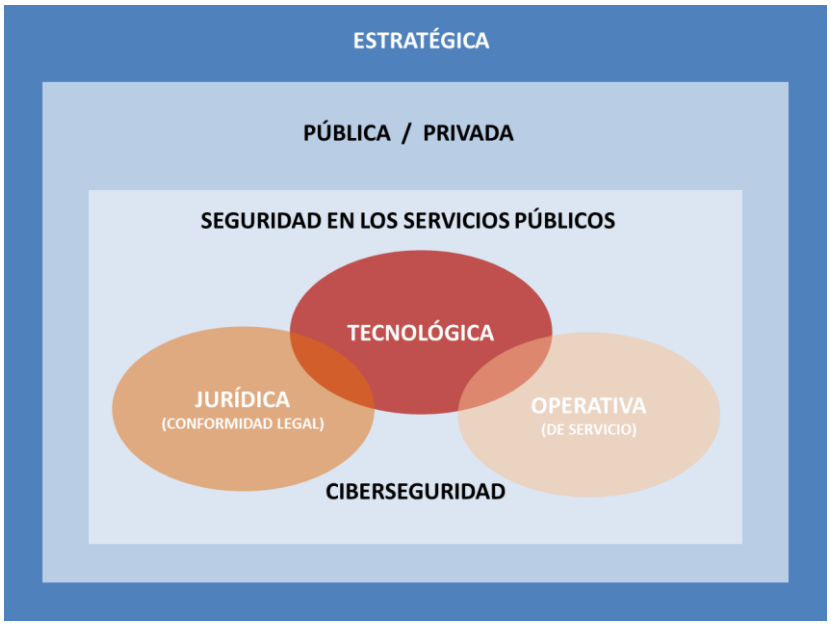

Figura 1. Las perspectivas de la ciberseguridad

Sin embargo, no siempre fue así.

Originariamente –años 60 del pasado siglo-, la que hoy podemos denominar como **"Seguridad Operativa"** o **"Seguridad ligada a los servicios"** constituyó el único concepto sobre el que pivotaba la seguridad en ambiente público-administrativo. La escasa utilización de los medios electrónicos en el desenvolvimiento del procedimiento administrativo significaba que la seguridad debía centrarse más en el respeto a los plazos y las formalidades del procedimiento que a los medios empleados en su desarrollo.

La irrupción, tímida primero, arrolladora después, de los medios electrónicos en las labores de las Administraciones Públicas dio lugar a la aparición de dos nuevas disciplinas que, conjuntamente con la anterior, estaban llamadas a configurar los pilares de la actuación administrativa automatizada. Nos estamos refiriendo a la **"Seguridad de los sistemas de información"**, también llamada en ocasiones **"Seguridad TIC"**, cuyo objeto de estudio es precisamente analizar y, a la postre, garantizar, que los servicios públicos, cuando son desarrollados o implementados a través de medios tecnológicos, poseen las suficientes garantías de seguridad que permiten considerarlos confiables, tanto para los ciudadanos –destinatarios últimos- como para las entidades prestadoras, y la **"Conformidad Legal"** con la regulación vigente: lo que hemos venido entendiendo como **"*Compliance* Tecnológico"** o **"Seguridad Jurídico-Tecnológica"**, cuando lo que se pretende es garantizar que las medidas tecnológicas y de otra índole que se adoptan en los servicios están amparadas y alineadas con un ordenamiento jurídico previo y habilitante, que regula su uso.

A este conjunto de elementos que configuran la seguridad en el tratamiento de la información y la prestación de los servicios públicos, cuando tienen lugar a través de instrumentos tecnológicos, electrónicos o digitales es lo que he denominado en este artículo **Ciberseguridad Pública**.

2. EL MARCO LEGAL DE LA CIBERSEGURIDAD.

La importancia que el legislador viene concediendo a la regulación pública de la Cibserseguridad tiene reflejo en la extensa normativa que, de un modo otro, pretende ordenar aspectos –necesariamente parciales- de la Ciberseguridad. La figura siguiente muestra, gráficamente, los aspectos más significativos de la complejidad y diversidad legal que sustenta la Ciberseguridad Pública en España.

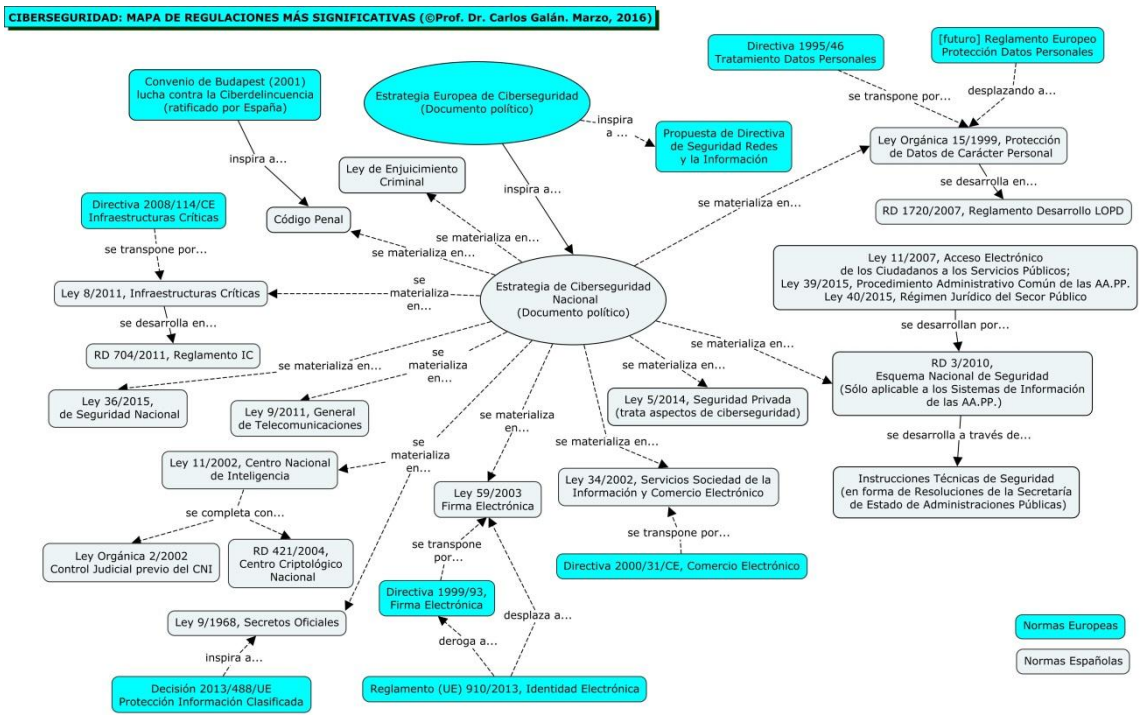

Figura 2. Legislación más significativa en materia de Ciberseguridad

El grado de interdependencia de las antedichas tres manifestaciones de la seguridad (tecnológica, jurídica y operativa) es tan importante, que, en muchas ocasiones, no es posible distinguir cuando un concepto concreto se encuentra situado dentro del dominio competencial de una (o varias) de ellas. Un caso claro lo encontramos, por ejemplo, en el concepto de "firma electrónica" que, además de constituir un elemento tecnológico en sí mismo es, al tiempo, un concepto jurídico y una garantía operativa.

3. SEGURIDAD PÚBLICA Y PRIVADA.

Por otro lado, independientemente de cuál fuera la seguridad finalista perseguida (tecnológica, jurídica u operativa), podemos refinar su ontología, clasificándola atendiendo también a los sujetos encargados de "construirla" o de "disfrutarla". Como en otros órdenes sociales o jurídicos, nos encontramos aquí con las vertientes pública y privada de la *generación* y la *recepción* de la seguridad.

Así, podemos hablar de entidades de naturaleza pública que, asimismo, prestan servicios de ciberseguridad a organismos públicos. Tal es el caso, por ejemplo, del **Centro Criptológico Nacional (CCN)**, dependiente del **Centro Nacional de Inteligencia (CNI)**, cuyas competencias y funciones en materia de ciberseguridad se dirigen, muy especialmente, a los sistemas de información de las entidades de las Administraciones Públicas y a aquellos sistemas que tratan información clasificada.

En otros casos, encontramos entidades de naturaleza pública que, a diferencia de la clase el anterior, dirigen su actividad al sector privado. Un buen ejemplo de ello es la expedición del nuevo DNI electrónico 3.0 a los ciudadanos españoles, en cuya emisión juega un papel central la **Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda**.

Los citados son tan solo un par de ejemplos representativos de los muchos que podrían mencionarse y que dan muestra del compromiso común de los sectores público y privado en materia de Ciberseguridad, cualquiera que sea su apellido: pública o privada.

4. LA SEGURIDAD ESTRATÉGICA.

Finalmente, no sería posible desarrollar de modo coherente las tres vertientes de la ciberseguridad que hemos venido señalando (tecnológica, jurídica y operativa) sin que exista un marco de actuación que propicie un desenvolvimiento ordenado de todas y cada una de ellas, no sólo a nivel nacional, sino también en relación con los países de nuestro entorno occidental y, muy especialmente, con los socios y aliados de España.

Recientemente, se ha cumplido el cuarto aniversario desde que, como consecuencia de la reunión de la Comisión Delegada del Gobierno para Asuntos de Inteligencia (CDGAI), celebrada el 1 de marzo de 2012, la Vicepresidencia del Gobierno encargó al Centro Nacional de Inteligencia la primera redacción de lo que, a finales de 2013 y tras un concienzudo proceso de mejora por parte de todos los organismos responsables, constituyó finalmente nuestra **Estrategia de Ciberseguridad Nacional (ECSN)**, bajo la superior dirección del **Consejo de Ciberseguridad Nacional.**

La publicación de la ECSN colocaba nuestro país en igualdad de condiciones con aquellos otros que, con anterioridad, habían determinado que el mantenimiento de una sociedad justa y próspera sólo podía realizarse si los sistemas de información de los que dependía poseían las debidas garantías que les permitieran hacer frente y recuperarse con presteza de los incidentes, deliberados o accidentales: lo que hemos venido denominando "***resiliencia***".

5. CNIS 2016: LA MESA DE LA SEGURIDAD.

Buena prueba del carácter poliédrico de la seguridad, genéricamente entendida, de los servicios públicos lo constituyeron las distintas ponencias que conformaron la Mesa Redonda del CNIS 2016, titulada genéricamente **"La Seguridad en los Servicios Públicos".**

Así, **D. Javier Candau**, Jefe de Área de Ciberseguridad del **Centro Criptológico Nacional**, centró su ponencia en la reciente actualización del **Esquema Nacional de Seguridad (ENS) -**un claro ejemplo de relación pública-pública-, como norma jurídica garante de la seguridad de la información tratada por las entidades públicas y los servicios por ellas prestados, actualización operada por la reciente publicación y entrada en vigor del Real Decreto 951/2015, de 23 de octubre, por el que se modifica el RD 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la administración electrónica.

Esta norma, el ENS, de obligado cumplimiento para todas las entidades públicas de cualesquiera de sus administraciones (General del Estado, de las Comunidades Autónomas o de las Entidades Locales) constituye el elemento regulador más importante de la Ciberseguridad Pública, siendo capaz de recoger los principios básicos y los requisitos mínimos sobre los que deben asentarse y a los que deben estar sometidos todos los sistemas de información de las entidades públicas de su ámbito de aplicación, en el desenvolvimiento de sus funciones.

Para facilitar la aplicación del ENS se han venido desarrollando, al amparo de las competencias que la ley atribuye al CCN, distintas **herramientas** (documentales y tecnológicas) destinadas a ayudar a los responsables públicos en la adecuada implantación de dicho ordenamiento, en todas las fases del ciclo de vida de los sistemas, desde la identificación y el análisis de los riesgos, hasta la preceptiva comunicación del estado de la seguridad de los sistemas afectados.

Por su parte, **Dña. Esther Muñoz**, Jefe de Área de Seguridad de Sistemas y Comunicaciones de la Subdirección General de Infraestructura y Operaciones, de la **Agencia para la Administración Digital de la Comunidad de Madrid**, señaló las actividades que se encuentra desarrollando en tal sentido el organismo al que pertenece, mostrando con claridad los más significativos retos a los que debe enfrentarse su organización, a saber: diseñar infraestructuras resilientes; potenciar las capacidades de prevención, detección, reacción, análisis, y respuesta; mejorar la coordinación ante incidentes; implementar una estrategia de defensa por capas y defensa en profundidad y renovar las infraestructuras obsoletas, actividades todas ellas enmarcadas también en una relación que podríamos definir como pública-pública.

El **Dr. Enrique Belda**, Subdirector General de Sistemas de Información y Comunicaciones para la Seguridad, de la **Secretaría de Estado de Seguridad del Ministerio del Interior**, en un claro ejemplo de relación pública-privada, mostró las características y cualidades de la galardonada aplicación ***AlertCops***, la primera aplicación para dispositivos móviles desarrollada para servir para comunicar a las Fuerzas y Cuerpos de Seguridad del Estado aquellas incidencias de las que los ciudadanos son víctimas o meros testigos. Se trata, pues, de un claro ejemplo en el que la tecnología, abandonando los recintos policiales, se introduce en el bagaje habitual del ciudadano para, al tiempo que facilita su actividad cotidiana y el cumplimiento de sus obligaciones, propicia la comunicación de los delitos que conduzcan a su ulterior persecución y detención y enjuiciamiento de sus autores.

Finalmente, **D. Valentín Ramírez**, Jefe de Área de la **FNMT-RCM**, presentó el nuevo **DNI electrónico 3.0** -un proyecto de tres años de duración-, un nuevo dispositivo de identificación que, mejorando y actualizando las características del anterior DNI, viene a facilitar su uso por parte de los ciudadanos, contribuyendo a diluir las barreras de entrada que toda tecnología conlleva. De nuevo, también en este caso, los dispositivos móviles cobran relevancia capital. Conocedores de que "si el futuro es móvil, la seguridad también habrá de serlo", la FNMT-RCM ha diseñado un dispositivo que, gracias a su interfaz NFC y a sus características tecnológicas, permite acceder de forma segura a los servicios de administración electrónica desde *smartphones* y *tablets*, facilitando la creación de pequeñas y sencillas aplicaciones que resuelvan de forma segura problemas cotidianos, tales como la firma de autorizaciones, consultas rápidas de datos, etc., Sin excluir ulteriores aplicaciones en proyectos de innovación dirigidos a Smart Cities y Smart Grids.

6. CONCLUSIONES.

De todo lo anterior podemos extraer varias conclusiones.

En primer lugar, como hemos visto, la Seguridad –también, la ciberseguridad- no es un concepto de fronteras perfectamente definidas. Muy al contrario, en su configuración intervienen, se superponen, se integran y, en ocasiones, se erosionan mutuamente, conceptos, métodos, procedimientos, herramientas y regulaciones que construyen una realidad multiforme y multidisciplinar.

En segundo lugar, la Ciberseguridad ya no es una opción. La dependencia de las sociedades occidentales de sus sistemas de información (públicos y privados) es de tal magnitud, que no puede abordarse ningún proyecto público que no contemple la seguridad de los sistemas de información, la información tratada y los servicios prestados, como requisitos tan importantes como la propia prestación de los servicios.

Y en tercer y último lugar, la seguridad -la ciberseguridad, también- no constituye una categoría absoluta ni, una vez alcanzada, admite alteración. Al contrario: la seguridad es un concepto limitado por los propios intereses sociales, políticos o económicos que la procuran en cada momento, del mismo modo que la mutación de aquellos intereses y el entorno cambiante en el que se asientan obligan a revisar cíclica -y eternamente, me temo- la naturaleza de los activos a proteger, los riesgos a los que están sometidos y las medidas de seguridad adoptadas para mitigarlos.

Los países más avanzados en materia de Ciberseguridad, entre los que ya se encuentra España, han diseñado estrategias nacionales (de repercusión internacional) tendentes a hacer frente a los retos que supone operar en el ciberespacio. De nuestra actividad, de nuestro celo, de nuestra profesionalidad, en suma, depende que los servicios públicos españoles, presentes y futuros, posean el adecuado nivel de confiabilidad que nos permita crecer como Estado, como ciudadanos y como personas.