CAPÍTULO I

La ciberseguridad como garantía de la continuidad de las funciones y servicios públicos locales en el mundo tecnológico

José Julio Fernández Rodríguez
Catedrático de Derecho Constitucional.
Universidad de Santiago de Compostela

Tamara Álvarez Robles
Prof.ª Permanente Laboral de Derecho Constitucional.
Universidad de León

1. Introducción

Es posible que muchos de los lectores no estén familiarizados con la historia de los primeros virus informáticos Creeper o Wabbit, en los años setenta del pasado siglo, ni con uno de los primeros *softwares* dañinos, conocido como gusano Morris, de finales de los años ochenta (Rodríguez, 2023). Empero, es probable que hayan leído o escuchado hablar de los *ransomware* Petya (2016) y WannaCry (2017) debido a la atención mediática que recibieron y al impacto que tuvieron en las Administraciones públicas y en las empresas, en una época en la cual los Estados ya habían iniciado su transición digital. Seguramente sean conocedores de la caída

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

que sufrió Microsoft a consecuencia de un fallo de seguridad de uno de sus proveedores, CrowdStrike, en julio de 2024, ampliamente difundida no solo por la repercusión en los medios de comunicación, sino preeminentemente por la paralización de los servicios públicos y privados a nivel mundial. A pesar de que la ciudadanía no está familiarizada con los nombres de estos virus —troyanos, *ransomware* y demás tipos de *malware*—, somos plenamente conscientes de los efectos perjudiciales que tienen en nuestro día a día. La ciberseguridad se configura, así, como una de las categorías esenciales para conseguir el progreso individual, social e institucional.

Sin duda, nos hallamos en un mundo convulso e incierto, en el cual el inusitado desarrollo tecnológico de las últimas décadas ha incidido en todos los órdenes de nuestra vida. Se ha conformado una nueva sociedad, la denominada "sociedad de la información", aunque también podríamos rotularla como "sociedad tecnológica", en la que ya nada será como antes. Incluso podemos hablar en la actualidad de un segundo momento de la sociedad de la información, determinado por el auge de las tecnologías disruptivas, como la inteligencia artificial, la computación en nube, el *blockchain*, la impresión 3D, la robótica, el 5G o, incluso, la computación cuántica. Un escenario abierto que justifica la incertidumbre a la que nos referíamos antes.

Debemos tener en cuenta que la tecnología es ambivalente y dicotómica, en el sentido de que presenta tanto elementos positivos como negativos. En el lado favorable encontramos, por ejemplo, las enormes posibilidades para la comunicación, el ocio y el comercio electrónico. En el lado negativo podemos situar las amenazas a la privacidad, la manipulación informativa, la ciberdelincuencia, el aislacionismo social o la banalización de la información. Esta realidad enfatiza la importancia de las cuestiones de ciberseguridad[1].

1. Usamos un entendimiento amplio de ciberseguridad, como las acciones, métodos e instrumentos para garantizar en soportes tecnológicos la confidencialidad, integridad, disponibilidad y autenticación de la información y de los servicios (seguridad en el mundo digital) (Fernández Rodríguez, 2018: 53). Sin embargo, hay conceptos más específicos, en los que la ciberseguridad se enfoca más en la protección de datos y sistemas interconectados, mientras que el concepto de seguridad de la información aborda un enfoque más holístico, incluyendo la gestión integral de la información y sus riesgos (Álvarez Robles, 2024a: 268). Aun así, optamos por dicha visión amplia: "La ciberseguridad será la seguridad del Estado tecnológico y del Estado tecnológico-digital. De este modo, atenderemos a una conceptualización de ciberseguridad integral (que va desde el Estado y sus Administraciones hasta los ciudadanos y empresas), transversal (que se proyecta en el sistema normativo, en las políticas públicas, en las normas técnicas, etc.) y descentralizada (en una visión internacional, supranacional [nacional] e infraestatal, con los principios de cooperación y colaboración como pilaras); a una ciberseguridad

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Como se ve, el tema resulta esencial, por lo que los poderes públicos deben prestarle la suficiente atención, con el ánimo de apoyar elementos positivos de la tecnología y mitigar los aspectos negativos. Sorprende que a veces los responsables públicos no muestren interés por esta problemática, ni la conozcan en sus elementos nucleares, ni sean conscientes de que cada vez presentará mayor trascendencia. En el ámbito local resulta incuestionable cómo la ciberseguridad debe situarse en la parte prioritaria de su agenda.

Podemos considerar que los ciberataques que sufrió Estonia entre el 27 de abril y el 18 de mayo de 2007 simbolizan el antes y el después de la ciberseguridad. Estos ciberataques tuvieron un profundo impacto en el normal funcionamiento del Estado estonio, de sus Administraciones y empresas, y en la vida cotidiana de sus ciudadanos. Estaban dirigidos contra los sistemas informáticos públicos y privados, y provocaron la disrupción y el bloqueo de las páginas web del Ejecutivo, del Legislativo, de distintas Administraciones, así como de los sistemas bancarios y medios de comunicación. Este suceso representó un punto de inflexión en la ciberseguridad, tanto del propio Estado estonio como a nivel supranacional —de la Unión europea— e internacional, con la implicación de la OTAN. A partir de ese momento la seguridad de la información evolucionaría hacia la ciberseguridad, ampliando sus horizontes más allá del ámbito estatal. Dentro del Estado se fortalecerían las capacidades de las Administraciones y empresas estratégicas y críticas, con el objetivo de garantizar la protección integral, y de continuar con las funciones y los servicios públicos frente a las ciberamenazas (Liga de Ciberdefensa de Estonia). A nivel internacional cobrarían fuerza los principios de cooperación y coordinación en la Unión Europea (Agencia de la Unión Europea para la Ciberseguridad) y en la OTAN (revisión del art. 5 del Tratado y Centro Integrado de Ciberdefensa).

En España, el incidente estonio, unido al incremento del 55 % en los ataques que se comenzaban a producir en los últimos años (CCN-CERT, *Principales Amenazas y Tendencias de la Seguridad Cibernética*, 2007)[2],

público-privada centrada en los sistemas de información, en y del ciberespacio (*security and safety)* y en los ciudadanos, cultura de ciberseguridad" (Álvarez Robles, 2024a: 269). En todo caso, el fin que ha de perseguir cualquiera de las acepciones de ciberseguridad, para ser continuista y evolutiva del concepto de seguridad, es la salvaguarda de los derechos y libertades, esto es, una ciberseguridad humanista.

2. https://www.ccn-cert.cni.es/es/comunicacion-eventos/comunicados-ccn-cert/1910-las-amenazas-y-vulnerabilidades-sobre-los-sistemas-de-informacion-se-incrementaron-un-55.html (fecha de última consulta: 01/12/2024).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

contribuyó a impulsar la creación de instituciones encargadas de velar por la ciberseguridad (Centro Nacional de Inteligencia, 2002; Centro Criptológico Nacional, 2004; CCN-CERT, 2006, y Consejo Nacional de Ciberseguridad, 2018), a legislar sobre protección de infraestructuras críticas (Ley 8/2011, de 28 de abril, de Protección de Infraestructuras Críticas) o sobre la conservación de datos (Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones), y a desarrollar estrategias de ciberseguridad (por ejemplo, Estrategia de Ciberseguridad Nacional 2013 y Estrategia Nacional de Ciberseguridad 2019).

Los ejemplos antedichos nos muestran una creciente preocupación por la seguridad, ciberseguridad, resiliencia y ciberresiliencia (DSN, *La Resiliencia en el Marco de la Seguridad Nacional*, 2024)[3], máxime cuando somos conocedores de que los fallos de seguridad y los ciberataques han evolucionado en cuanto a técnicas, métodos y actores implicados, y han aumentado en impacto a lo largo de los años (intensificándose en la pandemia de la COVID-19, según el Informe *Ciberamenazas y Tendencias*, edición 2020, del CCN-CERT)[4].

Estos ciberataques y fallos de seguridad nos hacen ser cada vez más conscientes de la interdependencia que tienen los sistemas y las sociedades (incluidas Administraciones), y han puesto de relieve el papel crucial del factor tiempo, tanto en la rápida propagación de estos eventos como en la urgencia de resolución de los mismos. Por ello, es primordial desarrollar una ciberseguridad que, además de proteger las infraestructuras críticas y estratégicas, se centre en los derechos de las personas y garantice una relación pacífica y armoniosa con las Administraciones públicas; una ciberseguridad que trascienda la visión tradicional que opone la Administración pública a la ciudadanía y que permita crear una verdadera cultura de ciberseguridad. A este relevante fin se dedica este capítulo.

En todo caso, vivimos tiempos de incertidumbre con relación al futuro, y también de cambios, que a nivel normativo, en el campo de la tecnología y ciberseguridad, provienen sobre todo de la Unión Europea (UE). La UE ha aprobado en los últimos años distintas normas que inciden en lo que estamos comentando de una forma u otra, aunque en términos de ciberseguridad debemos citar la Directiva UE 2022/2555, de 14 de di-

3. https://www.dsn.gob.es/sites/dsn/files/Resiliencia%20marco%20SN.pdf (fecha de última consulta: 25/10/2024).

4. https://www.ospi.es/export/sites/ospi/documents/documentos/Informe-Ciberamenazas-Tendencias_2020.pdf (consulta en diciembre 2024).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

ciembre, relativa a las medidas destinadas a garantizar un elevado nivel de ciberseguridad en toda la Unión (es la que se denomina Directiva NIS 2). Esta directiva debe ser transpuesta, lo que ha llevado a España a tener, en enero de 2025, un anteproyecto de ley de coordinación y gobernanza de la ciberseguridad[5].

2. La Administración local ante el mundo tecnológico: su papel central

2.1. La realidad de las amenazas y la necesidad de respuesta

Estonia fue, como mencionamos antes, el ejemplo más claro de cómo un Estado podía paralizar su normal funcionamiento por ciberataques coordinados. En este orden de cosas, y con relación a España, conviene señalar que desde el año 2006 el CCN-CERT ha asumido la gestión de más de 30 000 incidentes catalogados con un nivel de peligrosidad crítico o muy alto. Además, ha detectado 28 177 vulnerabilidades críticas con impacto en la seguridad de las tecnologías empleadas en el sector público; en la última década el número de incidentes gestionados anualmente por este organismo se ha incrementado un 1384,7 % (CCN-CERT, 23 de abril de 2024)[6]. A este número habría que sumar los ciberataques a empresas y otros organismos gestionados por el INCIBE-CERT y, en el marco de defensa, por el DEF-CERT, para tener un panorama completo.

El *ransomware* es el protagonista de gran parte de los ciberataques a entidades locales en estos últimos años. Así, podemos referirnos al troyano Emotet (especializado en el robo de datos financieros) en conjunción con el *ransomware* Ryuk, que afectó al Ayuntamiento de Jerez de la Frontera en octubre 2019[7] y cifró los archivos alojados en más de 50 servidores informáticos, paralizando, de este modo, los servicios del propio ayun-

5. La citada Directiva 2022/2555 (conocida con NIS 2) se aplica a las Administraciones públicas centrales y regionales (art. 2.2.f), aunque también deja la puerta abierta a los Estados para que amplíen esta previsión a la Administración local (art. 2.5.a). En el anteproyecto español de transposición que se conoce en febrero de 2025 no se realiza tal posibilidad (en su anexo 1, punto 10, las entidades de la Administración pública son tan solo las centrales y regionales). Este anteproyecto se puede consultar en https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/participacion-ciudadana/Participacion-publica-en-proyectos-normativos/Audiencia-e-informacion-publica/01_2025_Anteproyecto_ley_coordinacion_gobernanza_ciberseguridad.pdf.

6. https://www.ccn-cert.cni.es/es/seguridad-al-dia/actualidad-ccn/12943-el-centro-criptologico-nacional-ha-gestionado-mas-de-30-000-ciberincidentes-de-peligrosidad-muy-alta-y-critica-en-sus-20-anos-de-trayectoria.html#:~:text=El%20pasado%20a%C3%B1o%2C%20el%20CCN,incrementado%20un%201.384%2C7%25 (última consulta: 01/12/2024).

7. Este *ransomware* sería el introducido en el Servicio Público de Empleo Estatal-SEPE en 2021. Recordemos que tres meses más tarde se produjo un ciberataque a distintas secciones

tamiento junto a otros servicios públicos dependientes de este. En esa época fuimos testigos de sucesos similares: en noviembre de 2019 se vería afectado el Instituto Municipal de Empleo y Fomento Empresarial del Ayuntamiento de Zaragoza, por el secuestro de información. Los Mossos informaron durante 2020 de diferentes ciberataques en ayuntamientos tales como Guixers, Lliçà de Vall, L'Escala y Sant Just Desvern. La operación Oceansx, de la Guardia Civil, reveló cómo, desde octubre de 2022, se perpetraron distintos ataques a organismos públicos: ayuntamientos de León y Salamanca, y diputaciones de Jaén y Málaga. Ese mismo año 2022, la Asociación Navarra de Informática Municipal comunica la caída de sus servidores (webs, correos y sedes electrónicas inutilizadas), con Hive y Cobalt Strike, afectando a 137 ayuntamientos y 35 entidades navarras. El año 2023 se estrenaría, a finales de enero, con el ciberataque a la Diputación Foral de Vizcaya, lo que desactivó los servicios de su sede electrónica. Este ciberataque afectó a la gestión interna de los ayuntamientos integrados en la red de BiscayTIK, 107 de los 112 ayuntamientos de Vizcaya. A mediados de año, en junio de 2023, Lockbit visitaría el Concello de Cangas (Galicia), que vería cómo la mitad de los ordenadores quedaban paralizados, afectando, entre otros, a la gestión y al pago de las nóminas de 229 empleados; mientras que en septiembre atacó los servicios informáticos del Ayuntamiento de Sevilla, dejando su sede electrónica inutilizada y reclamando 5 millones de euros. Granada, en octubre de 2023, sería objetivo del grupo criminal NoName057[8], afectando al normal funcionamiento de las webs del transporte urbano del Ayuntamiento. El Ayuntamiento de Torre Pacheco sería víctima de un *ransomware* en abril de 2024, en el que se vio comprometida información sensible de los ciudadanos y procedimientos administrativos. Tampoco se libraría el Ayuntamiento de Benalmádena, cuyo sistema de cita previa se vio afectado en junio de 2024[9].

De todo lo anterior podemos inferir que los ciberataques son habituales en el ámbito local y que existen diversos tipos de ciberataques que

de la Sede Electrónica de la web del Ministerio de Trabajo, afectando a organismos dependientes, como las consejerías de Trabajo.

8. Presuntamente, el mismo grupo criminal que perpetró ciberataques a distintas webs estatales en la época de las elecciones generales españolas. El referido ataque a Granada se produjo cuando en esa ciudad se celebraba una cumbre europea de jefes de Estado y de Gobierno, lo que denota el interés geopolítico de este grupo de ciberatacantes.

9. Mismo año en el que varias webs de hospitales pertenecientes al Servicio Andaluz de Salud vieron afectado su normal funcionamiento. En efecto, el 9 de julio se detectó en los hospitales universitarios Clínico San Cecilio y Virgen de las Nieves, y en el Área de Gestión Sanitaria Sur de Granada y Distrito Sanitario Granada-Metropolitano, un incidente de seguridad que afectó a las páginas web de dichos hospitales, pero no a la infraestructura, servicios o datos personales de empleados o usuarios.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

pueden afectar gravemente a los servicios de un ayuntamiento, comprometiendo la seguridad de la información y la continuidad de sus servicios. Incluso se puede sostener que hemos asistido a un incremento de los ciberataques dirigidos específicamente contra las entidades locales. Muchas entidades locales están migrando servicios a la nube, lo que conlleva nuevos desafíos de ciberseguridad relacionados con el almacenamiento de datos, la seguridad de las plataformas y el control de acceso. También la aparente debilidad que se refleja en el ámbito local estimula las amenazas.

Los protagonistas de los ciberataques suelen ser estos tres: el *malware* en general[10], el *ransomware*[11] y el *phishing*[12]. Al ser los ayuntamientos responsables de servicios esenciales (agua, saneamiento, gestión de residuos, pagos, servicios sociales, etc.), los ataques de *ransomware* (cifrando datos y exigiendo un rescate) pueden tener consecuencias graves. A su vez, los ataques de *phishing* también son un riesgo importante, ya que los empleados municipales pueden ser víctimas de correos electrónicos fraudulentos que comprometen sus credenciales o permiten la instalación de *malware*. En todo caso, es habitual que el éxito del ataque acabe afectando directamente a la población.

En otras ocasiones la amenaza a la que se enfrentan los consistorios se dirige contra sus dirigentes. Este tipo de amenazas, que forman parte de campañas hibridas, lo pudimos observar con el *deepfake* al alcalde de Madrid en junio de 2022. De esta forma, se consiguió suplantar la identidad de su homólogo ucraniano de la ciudad de Kiev, Vitali Klitscko. Esta

10. El *malware* puede afectar a los servicios de un ayuntamiento partiendo de un troyano diseñado para infiltrarse en los sistemas informáticos municipales. Este tipo de *malware* se oculta en un archivo aparentemente inofensivo, como un documento o una aplicación que un empleado descarga sin sospechar nada. Una vez dentro del sistema, el troyano puede abrir una puerta trasera que permite a los atacantes acceder de manera remota a la red interna del ayuntamiento. Desde allí, los ciberdelincuentes pueden robar datos sensibles, como información personal de los ciudadanos, registros de impuestos o expedientes confidenciales.

11. Uno de los ataques más comunes en estos últimos años es el *ransomware*, un tipo de *malware* que cifra los archivos de los sistemas informáticos y exige un rescate para su liberación. Hemos podido comprobar que se han parado servicios como los de petición de citas, pagos a empleados, la recaudación de impuestos o el acceso a documentos públicos, afectando gravemente la prestación de servicios a sus ciudadanos.

12. Una técnica bastante utilizada es el *phishing*: los empleados municipales son engañados a través de correos electrónicos o mensajes fraudulentos, con enlaces o archivos maliciosos, permitiendo a los atacantes infiltrarse en las redes internas y acceder a información. Esto no solo compromete la seguridad de la información, sino que también pone en riesgo la integridad de servicios como la tramitación electrónica de expedientes o el sistema de atención al ciudadano, lo que podría conllevar la alteración o el robo de datos personales y la interrupción de procesos administrativos clave.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

acción usó inteligencia artificial e hizo pensar que se estaba manteniendo una conversación en tiempo real que resultó ser falsa. En realidad no hubo daños, pero se sembró la desconfianza en este tipo de videoconferencias.

Estos son solo unos pocos ejemplos ilustrativos de cómo las Administraciones y los organismos públicos locales han padecido las consecuencias de los ataques realizados por un enemigo silencioso y elusivo que, a través de distintos mecanismos, busca alterar su normal funcionamiento. A ello se han de añadir los errores derivados de la ausencia de políticas de seguridad de la información, o de una inadecuada implementación de las mismas. Como se ha podido comprobar, las Administraciones han sido objeto de distintos ataques producidos por la ciberdelincuencia (*malware*, *ransomware*, *phishing*, ingeniería social, explotación de vulnerabilidades, denegación de servicios, accesos no autorizados a información, suplantaciones); también han tenido que enfrentarse al *hacktivismo* personas que han tenido información privilegiada, al espionaje y a distintos errores y daños físicos (fuego, agua, cortes de suministro)[13]. Estas anomalías han impedido el normal funcionamiento de los servicios municipales, incidiendo directamente en la vida diaria de los ciudadanos, que no han podido realizar sus trámites administrativos, han visto cortados los suministros, no han recibido la ayuda social a tiempo, o han visto cómo se hacían públicos datos de carácter personal.

En suma, del análisis de lo anterior se puede derivar la existencia de varios tipos de ataques en función del daño que sufren los consistorios: por un lado, el cifrado y robo de la información usando *ransomware* supone una doble extorsión y causa graves daños, por cuanto afecta a la disponibilidad de los datos y suele implicar perjuicios económicos; por otro, se producen robos de información que termina vendiéndose en la *dark web*, y cuya protección depende en gran medida de las copias de seguridad (que se tengan, que estén disponibles, que estén actualizadas); asimismo, hay ataques de denegación de servicio (*DDoS*), que suelen tener un menor impacto porque, en principio, se podría recuperar el servicio fácilmente una vez que se identificase la procedencia del ataque; o aquellos que tratan de afectar a la confianza de la sociedad por estar dirigidos contra una persona determinada, sin llegar a poner en riesgo el conjunto de la actividad del ayuntamiento, pero que demuestran la interrelación entre la seguridad de la información y la ciberseguridad de los dirigentes con la

13. Para mayor información, nos remitimos al *Prontuario de ciberseguridad para entidades locales*, fechado en abril de 2021, del Centro Criptológico Nacional y la Federación Española de Municipios y Provincias.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

propia Administración (incluidos sus dispositivos personales, dada la información sensible que pueden manejar). De este modo, la imagen municipal se deteriora y, por ende, se incrementa la desconfianza ciudadana. Y, subsiguientemente, incluso asistiríamos a un coste electoral para el partido que gobierna la entidad, y se atraerían más ataques al dar muestras de debilidad tecnológica.

Hay que tener presente, como decimos más abajo, que las entidades locales tanto deben garantizar los derechos fundamentales en el entorno digital actual como prestar servicios a su ciudadanía, los cuales en gran parte ya dependen de una infraestructura tecnológica. De este modo, resultan esenciales la atención que debe prestar y el trabajo que debe realizar la Administración local en ambos sentidos. La ciberseguridad no es una elección para los entes locales, al contrario, ha de ser considerada una prioridad en una sociedad comprometida con la digitalización. Este esfuerzo tiene que comenzar con el máximo representante de la corporación (el alcalde) y extenderse a todos los niveles de la institución (incluyendo a todos y cada uno de los empleados y miembros de la corporación, y a las empresas que le prestan servicios). La ciberseguridad debe ser el eje que oriente la implementación de los sistemas y tecnologías que se instalen (tanto a nivel *hardware* como *software*), una verdadera cultura de funcionamiento que hay que integrar en la dinámica cotidiana de los entes locales.

En definitiva, la realidad de las crecientes ciberamenazas lleva a la imperiosa necesidad de que las Administraciones locales se protejan frente a ellas, con una respuesta bien planificada en sus vertientes estratégica, táctica y operativa. De esta forma, tal respuesta garantizará los pilares de confidencialidad, integridad y disponibilidad de la información, ejes nucleares de esta problemática.

2.2. Las oportunidades de las características de la Administración local

En este escenario incierto y convulso por el que transitamos en el siglo XXI, la Administración local desempeña un papel clave. Sus propias características así lo determinan, provocando la necesidad de que las entidades locales afronten de manera decidida y efectiva el desafío que marca el mundo tecnológico. Los rasgos de las entidades locales se convierten en una oportunidad para que jueguen ese rol trascendental que estamos comentando. Es decir, tales características son elementos oportunos, convenientes y favorables para que avance la ciberseguridad en el predio local,

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

lo que no significa que ello suceda automáticamente, ya que se deben realizar distintas acciones que veremos más adelante, en el apartado 6.

Con base en la premisa apuntada, abordamos a continuación estos elementos que determinan el citado papel central. Como se verá, se trata de cuestiones conectadas unas con otras que en algunos de sus aspectos se solapan.

En primer lugar, la **autonomía** de los entes que conforman la Administración local les debe permitir organizar de forma adecuada las respuestas que hay que articular frente al desafío tecnológico, lo que tiene que incluir un plan propio para la ciberseguridad. La autonomía local posibilita una respuesta ágil y adaptativa a los desafíos tecnológicos, dado que esta autonomía les otorga competencias propias, capacidad de gestión y de decisión en el ámbito propio, así como la posibilidad de implementar políticas y estrategias alineadas con las necesidades específicas de sus comunidades. En este sentido, la autonomía refuerza la cercanía a la ciudadanía, la gestión eficiente de recursos al permitir que las entidades locales prioricen la inversión en tecnologías específicas, el fomento de la participación ciudadana digital, la colaboración público-privada y la resiliencia frente a los riesgos tecnológicos. Resulta imprescindible que esta autonomía se emplee para desarrollar políticas específicas de ciberseguridad y protección de datos, necesarias en un contexto donde los riesgos tecnológicos, como ciberataques o el uso indebido de datos personales, son cada vez más relevantes. Así será también en el futuro.

Además, las entidades locales tienen **competencias específicas** que destacan por su **proximidad a la ciudadanía**, lo que las convierte en actores clave en la prestación de servicios y la gestión de recursos a nivel social. Estas competencias están definidas en la legislación y varían según el marco normativo de cada país, pero suelen incluir servicios básicos esenciales (que comentamos después); bienestar social y comunitario, con servicios sociales como la asistencia a personas mayores y personas con discapacidad o en riesgo de exclusión social; atención a situaciones de vulnerabilidad social; gestión de ciertos aspectos de los servicios educativos, como escuelas infantiles o actividades extraescolares; urbanismo y medio ambiente (gestión del suelo, parques, jardines, zonas verdes, promoción de la movilidad sostenible); cultura, deporte y ocio (organización de actividades de esta índole, gestión de bibliotecas, centros culturales y polideportivos, promoción del turismo local y la conservación del patrimonio histórico); seguridad y protección ciudadana (policía local, protección civil, emergencias); y fomento económico y empleo (apoyo a pequeñas y

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

medianas empresas locales, promoción del empleo mediante programas de formación y desarrollo local).

Estas competencias, y la propia proximidad geográfica y administrativa de las entidades locales a la población, les permiten actuar de manera más rápida y adaptada a las necesidades concretas de sus comunidades, fomentando la participación ciudadana y la implementación de políticas orientadas al desarrollo local sostenible. Las entidades locales, gracias a su proximidad, pueden comprender mejor las demandas y expectativas de los ciudadanos en cuanto al uso de nuevas tecnologías. Esto permite respuestas más personalizadas y rápidas, como la digitalización de trámites administrativos o la creación de aplicaciones para reportar problemas urbanos en tiempo real.

A mayor abundamiento, las competencias sobre los **servicios públicos básicos** enfatizan lo dicho. Nos referimos a suministro de agua potable, alcantarillado y gestión de residuos; alumbrado público, pavimentación y mantenimiento de calles; o gestión de cementerios y servicios funerarios. Los servicios públicos básicos pueden ver mejorada su eficiencia con el apoyo tecnológico, lo que redundará en beneficio de la ciudadanía. Los entes locales deben trabajar en ello de manera correcta para que esta oportunidad se concrete en verdadera ventaja.

Los elementos de **financiación propia** explican también esta posición central de las entidades locales para asumir el reto tecnológico y los desafíos emergentes ligados al mismo, como la ciberseguridad. El marcado carácter mercantilizado y economicista de nuestro mundo demuestra lo imprescindible que es poseer recursos para cumplir las funciones propias. Este financiamiento permite que los Gobiernos locales dispongan de recursos suficientes para implementar políticas, programas y medidas que aseguren servicios públicos eficientes, la protección de datos de los ciudadanos y la resiliencia ante amenazas digitales. Una financiación adecuada posibilita recursos que se pueden emplear directamente en áreas prioritarias como salud, educación, infraestructura y digitalización de servicios. Esta autonomía es esencial para financiar plataformas tecnológicas que faciliten el acceso a derechos, como trámites en línea, consultas ciudadanas y servicios públicos digitales. Al mismo tiempo, disponer de recursos propios permite a los Gobiernos locales modernizar su infraestructura tecnológica, lo que incluye las medidas de ciberseguridad. La financiación otorga resiliencia frente a riesgos cibernéticos, como invirtiendo en auditorías de seguridad y formación especializada para el personal. También fomenta la inclusión digital: se reduce la brecha digital, al

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

promover el acceso equitativo a tecnologías y servicios en línea; y da flexibilidad en la implementación de soluciones locales, diseñando respuestas específicas a los desafíos tecnológicos y de ciberseguridad que enfrentan sus comunidades, en lugar de depender exclusivamente de recursos centralizados o transferencias condicionadas.

La **capacidad de adaptación** es otro elemento para considerar y que, de nuevo, refleja el papel central de la Administración local frente al desafío tecnológico. La capacidad de adaptación de las entidades locales frente a este desafío radica en su flexibilidad administrativa, la cercanía ya comentada con la ciudadanía y su posibilidad de diseñar políticas específicas en función de las necesidades locales. Además, también son factores de estas posibilidades de adaptación la autonomía de gestión, la colaboración con otras entidades o empresas para establecer alianzas estratégicas en transformación digital, el cierto grado de flexibilidad normativa, las alternativas en formación y capacitación, o la posible promoción de la participación ciudadana. Esta capacidad permite implementar soluciones innovadoras y enfrentar los retos tecnológicos de manera eficiente, lo que siempre debería tener como objetivo la mejora de la calidad de los servicios públicos y la garantía de los derechos fundamentales en un entorno digital.

En fin, además de lo dicho, también vemos de forma más general, al margen del tema tecnológico, que la Administración local es un agente esencial en la **protección de los derechos fundamentales**, sobre todo por esa posición comentada de cercanía a las personas y de asunción de servicios públicos básicos. Incluso esa garantía de derechos viene de la mano del papel que tienen que jugar las entidades locales en términos de ciberseguridad. Por lo tanto, no solo las específicas cuestiones de ciberseguridad, sino también el papel de estas entidades desde una perspectiva más general en la defensa de los derechos, subraya su trascendencia en lo que ahora nos ocupa.

3. La ciberseguridad como garantía de los derechos fundamentales

La ciberseguridad se ha convertido en una garantía de los derechos fundamentales. Ello puede parecer una afirmación atípica desde la dogmática jurídica de estos derechos, en donde se suele distinguir entre garantías normativas, jurisdiccionales e institucionales. No obstante, aun partiendo de tal construcción, semeja conveniente completarla con otras visiones más amplias, pues las diversas amenazas que se ciernen sobre los derechos aconsejan tal aproximación. A esto nos referimos cuando afirmamos

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

que la ciberseguridad se ha convertido en una garantía esencial para la protección de los derechos, asediados por diversos aspectos negativos de la tecnología. Para ilustrar estos extremos nos referimos a continuación a varios derechos, aunque lo hacemos en una aproximación escueta para no dilatarnos en demasía.

Para entender esta cuestión más cabalmente recordemos, como ya publicamos en su momento (Fernández Rodríguez, 2020), que el encuentro entre derechos y tecnología se puede ver desde la óptica del pasado, del presente o del futuro. Es decir, desde la visión de los derechos que hemos recibido (los derechos del pasado), los que se están creando a raíz del progreso tecnológico (derechos del presente), y los que posiblemente se plantearán en el futuro mediato o lejano (derechos del futuro). Con respecto a los **derechos del pasado** comentamos lo siguiente desde la óptica de la ciberseguridad:

– En primer lugar, la ciberseguridad sirve para mantener nuestra privacidad. El mundo tecnológico ha originado múltiples problemas para los derechos ligados a la privacidad o intimidad, como el derecho al honor, la propia imagen, la protección de las comunicaciones, la protección de domicilio o la protección de datos. Se trata de derechos diferentes, como objetos propios, pero que ahora los podemos conectar para ilustrar las amenazas tecnológicas en este ámbito. Ahí tenemos herramientas diseñadas en gran parte para atacar la intimidad, como virus, troyanos, gusanos, *ransomware*... *Malware* en general que refleja ese lado negativo de la tecnología. De esta forma, nos topamos con interceptaciones de *mails*, entradas en el disco duro sin consentimiento, suplantación de personalidad, perfilado de personas, *spam*, denegación de servicios, bloqueo de equipos informáticos, etc. Los datos se destruyen, se modifican, se fabrican o se roban. Al mismo tiempo, la tecnología también presenta una cara amable y ofrece herramientas de respuesta, como antivirus, cortafuegos, programas antiespía o antispam, criptografía. Por lo tanto, la implementación de correctas medidas de ciberseguridad es imprescindible y lo será cada día más. Una protección robusta de nuestros datos personales solo es en la actualidad posible con niveles avanzados de ciberseguridad.

– De igual forma, los derechos ligados a las libertades comunicativas también se hallan muy afectados en el mundo digital. Nos referimos a las libertades de expresión e información, y a las opciones y los derechos de participación posibilitados por tales libertades.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

La tecnología ha creado un ecosistema desinformador que se ha expandido por doquier. Ya antes existía manipulación informativa, obviamente, pero ahora las posibilidades de expansión tecnológica nos sumen en un momento diferente. Por un lado, la tecnología posibilita el envío masivo y automatizado de *fake news* por distintos soportes, sobre todo por las redes sociales; por otro, la inteligencia artificial generativa produce por sí misma estas noticias falsas con un realismo casi insuperable (texto, imágenes, sonidos). Así, se dificulta sobremanera el control que la opinión pública debería ejercer sobre el poder, y se plantean trabas para la limpieza del proceso electoral, en el que el votante puede no tomar libremente su decisión al estar seducido por los sesgos que lo engañan. De esta forma, nos hemos planteado si la manipulación informativa destruirá o no a la democracia (Fernández Rodríguez, 2024). Este problema se ha convertido en un verdadero reto ante el que debemos reaccionar con distintas medidas, entre las cuales se encuentran acciones de ciberseguridad que sirvan para detectar las *fake news* y realizar labores de contrapropaganda.

– Los derechos de participación política, como el derecho de sufragio, son ejercidos cada vez en más lugares por medio de instrumentos digitales, entre los que destacan las urnas electrónicas y las votaciones en línea. La ciberseguridad, en todo caso, debe ser robusta para evitar ataques que imposibiliten esta participación e, incluso, alteren el resultado electoral. Los sistemas de votación electrónica y las plataformas de consulta ciudadana requieren, por lo tanto, una ciberseguridad adecuada para afrontar los riesgos de las interferencias externas y los fraudes. Solo así habrá confianza ciudadana en las instituciones, y solo así el intercambio de ideas será más libre y seguro. Debemos tener garantías suficientes para asegurar los elementos distintivos del voto democrático: un voto universal, libre, igual y secreto.

– El derecho de tutela judicial emplea distintos soportes digitales en el marco de una administración electrónica judicial que ya incluye la presentación de demandas, las comunicaciones o la gestión de muchas pruebas y peritajes. Para que todo ello funcione con garantías es imprescindible un nivel de ciberseguridad adecuado, lo que de nuevo se revela como una garantía para el correcto ejercicio de la tutela judicial. En este sentido, en un trabajo de hace algunos años sosteníamos que los progresos técnicos son herramientas que se emplean para "conseguir los objetivos de impartición justa y rec-

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

ta de la justicia", y que la presencia del derecho fundamental de tutela judicial "exige especial intensidad en la implementación del e-gobierno en sede jurisdiccional" (Fernández e Iglesias, 2012: 75).

– También los distintos derechos sociales se ven protegidos por la ciberseguridad. Pensemos en la garantía del funcionamiento de la atención sanitaria, evitando ataques a sus sistemas; o en el suministro de productos de primera necesidad, como el agua o los alimentos, que puede verse truncado por la actuación de ciberdelincuentes. Sin embargo, el mayor reto es para los consumidores, objetivo habitual de los ataques informáticos con la intención de venderles productos fraudulentos, robarles datos o imponerles toda suerte de engaños. Incluso se han conformado técnicas sociales de ataque para ganar en persuasión (el ya comentado *phishing*). La ciberseguridad es, de igual modo, esencial en las actividades de consumo ante este amenazante panorama en el mercado digital.

Con relación a los **derechos del presente**, estamos asistiendo a la aparición de unos derechos nuevos ligados al desarrollo tecnológico, para los que se habla de derechos de cuarta generación. En este sentido, el más destacado en lo que ahora nos interesa es un derecho a la seguridad digital. Así, el art. 82 de la Ley Orgánica 3/2018, de protección de datos personales y garantía de los derechos digitales, prevé que "los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet". De esta forma, la ciberseguridad se convierte en el contenido de uno de los nuevos derechos que aparecen en el desarrollo tecnológico de estas décadas. Además, existen otros derechos ya contemplados expresamente, como el derecho de neutralidad de internet (art. 80 de la citada LO 3/2018) o el derecho de acceso universal (art. 81 de esta LO 3/2018), que evidencian las muchas novedades que trae el progreso tecnológico en este campo (Álvarez Robles, 2024b).

Por último, parece claro que el **futuro** supondrá la aparición de nuevos derechos que todavía están sin perfilar, pero que seguramente se ligarán, entre otros, a los derechos de los robots o de las personas transhumanas (Fernández Rodríguez, 2023). Además, se hará necesario precisar neuroderechos para proteger nuestro cerebro y pensamiento (como derechos de identidad digital, de libre albedrío, de privacidad digital, de acceso equitativo o de protección frente a los sesgos). Por lo tanto, ante este incierto e intenso futuro en el campo de los derechos, la ciberseguridad tendrá un creciente papel para que los nuevos desarrollos en este terreno puedan ser satisfactorios y no suponer una involución.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Con los distintos ejemplos de derechos mostrados en los párrafos precedentes creemos que corroboramos la afirmación que hemos empleado al inicio de este apartado: la ciberseguridad es una imprescindible garantía para los derechos en el mundo presente y futuro. Como las entidades locales deben también proteger los derechos de las personas, se ven obligadas indefectiblemente a apostar por un nivel suficiente de ciberseguridad.

4. Ciberseguridad y continuidad de los servicios y funciones de las entidades locales

Además del rol de las entidades locales en términos de ciberseguridad para proteger derechos, de igual manera un correcto entramado de ciberseguridad es imprescindible para asegurar que los servicios y funciones de esas entidades locales se desarrollen con normalidad. Por eso hablamos de garantía de la continuidad de estos servicios municipales, lo que de nuevo evidencia la relevancia actual y futura de la correcta gestión de las cuestiones relacionadas con el progreso tecnológico. Por todo ello consideramos que la protección de los municipios resulta esencial, debido al tipo de servicios que deben prestar a sus habitantes.

La ciberseguridad se revela como un componente crítico para garantizar esta continuidad de los servicios y funciones esenciales de las entidades locales. Recordemos que en España, según el art. 26 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, los municipios han de prestar una serie de servicios a sus ciudadanos, que en la actualidad pueden presentar relevantes vulnerabilidades ante ciberataques. Así, en la línea de lo apuntado antes en el apdo. 2.2, encontramos aquellos servicios que deben proveer con independencia de su tamaño: alumbrado público, cementerio, recogida de residuos, limpieza viaria, abastecimiento domiciliario de agua potable, alcantarillado, acceso a los núcleos de población y pavimentación de las vías públicas. Si la población es superior a 20 000 habitantes se incluyen protección civil, evaluación e información de situaciones de necesidad social y atención inmediata a personas en situación o riesgo de exclusión social, prevención y extinción de incendios e instalaciones deportivas de uso público. E incluso transporte colectivo urbano de viajeros y medio ambiente urbano, para aquellos municipios con una población superior a 50 000 habitantes.

Por lo tanto, estas instituciones manejan infraestructuras y datos sensibles que sustentan servicios básicos, como el suministro de agua, electricidad, transporte, educación y salud, así como funciones adminis-

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

trativas vitales. Es más, en la actualidad gran parte de estos servicios públicos municipales dependen de sistemas digitales, como el alumbrado público o la recolección de residuos. Por lo tanto, una brecha en la seguridad cibernética podría interrumpir significativamente estas operaciones, con consecuencias graves, tanto a nivel institucional como en el predio de la ciudadanía. Estos servicios dependen en gran medida de la administración electrónica, de la infraestructura tecnológica, que implica un manejo masivo de información, considerada el petróleo del siglo XXI. No obstante, esta acumulación de datos (en ocasiones sensibles) y su tratamiento por parte de empleados, quienes son el eslabón más débil de la cadena de seguridad, pueden aumentar la superficie de ataque y las vulnerabilidades a distintos tipos de ataques (en especial los relativos a la ingeniería social o *phishing*). Estas amenazas ponen en riesgo la integridad de los sistemas municipales y requieren la implementación de medidas y controles, de políticas de seguridad adecuadas para salvaguardar tanto la información como la propia infraestructura tecnológica por la que discurren los servicios municipales, activos tangibles e intangibles.

En este sentido, las entidades locales administran sistemas que forman parte de infraestructuras críticas, como plantas de tratamiento de agua y sistemas de transporte. La ciberseguridad asegura que estos sistemas sean resistentes a ataques que podrían causar interrupciones masivas. Es fácil imaginar de manera aquilatada la necesidad de esta ciberseguridad en, por ejemplo, el suministro de agua. Pensemos en las consecuencias de un sabotaje a los productos químicos que se vierten a la misma o en qué sucedería si no nos llegase agua, o si se rompiesen las bombas de agua. Otro ejemplo evidente es el caso de un apagón de los semáforos de la ciudad o si se ponen todos en verde. Dado que estas infraestructuras dependen en gran medida de tecnología interconectada y, además, son gestionadas por empleados que podrían ser objetivo de ataques, es crucial que se establezcan medidas de protección robustas para garantizar su funcionamiento continuo y la seguridad de la información manejada.

Igualmente, de nuevo debemos tener presente la temática de los datos personales. Las entidades locales almacenan información personal de los ciudadanos, incluidos datos sensibles que están presentes en impuestos, servicios sociales, registros de salud y empadronamiento o permisos. La ciberseguridad protege esta información contra accesos no autorizados y robos, que se convierten en uno de los principales desa-

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

fíos para garantizar los principios de seguridad de la información (acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de datos, información y servicios), en consonancia con sus respectivas competencias y para la adecuada prestación de los servicios.

De esta forma, la respuesta ante emergencias digitales en el ámbito local es clave para desactivar estos incidentes cibernéticos y restaurar rápidamente los servicios en caso de un ataque, lo que deberá incluir sistemas de respaldo y recuperación de datos. Pero tan importante como ello será la planificación previa desde una lógica proactiva, a lo que nos referimos más abajo en el punto 6.

Así las cosas, la ciberseguridad también se revela como un factor esencial para mantener la confianza en los servicios públicos. Las grietas en estas garantías materializan riesgos y amenazas que afectan a la vida diaria de la ciudadanía[14]. La interrupción de los sistemas municipales y la imposibilidad de prestar servicios con normalidad pueden tener consecuencias graves para la operatividad o el normal desarrollo de la actividad de los ayuntamientos, y para la vida diaria de la ciudadanía. Como hemos podido ejemplificar, estos incidentes (debidos a fallos y ataques) de ciberseguridad no solo generan retrasos en la prestación de servicios, sino que también pueden conllevar la percepción de inseguridad y la pérdida de confianza en las autoridades e instituciones locales. La desconfianza deriva en una percepción de inseguridad que a su vez desencadena quejas, malestar, e incluso ansiedad o miedo ante lo tecnológico-digital, ante la administración electrónica.

5. Obstáculos en las entidades locales para afrontar los retos de la ciberseguridad

14. No es difícil imaginar problemas realistas: el ayuntamiento ha sido víctima de un ataque y no se pueden conseguir copias del padrón municipal, lo que se exige en distintos trámites (como el del DNI); o la necesidad de acceder a un listado de ayudas sociales que se encuentra encriptado por un *ransomware*, y esa falta de acceso imposibilita el cobro de cierta ayuda; o la afectación del servicio municipal de transportes provoca retrasos para llegar al colegio, trabajo o citas médicas (lo que se puede producir en un momento en el que se depende del transporte público, ya que la ciudad tiene restringido el tráfico privado por estar celebrándose una cumbre de jefes de Estado); incluso, en alguna ocasión, hemos comprobado cómo el pago de las nóminas de los empleados municipales no se pudo realizar en tiempo y forma, con las consecuencias que ello puede tener para quien ha de realizar el pago del alquiler o hipoteca y los demás gastos corrientes y habituales. Pero más peligroso sería que se ponga en riesgo la integridad física, alterando los semáforos de la ciudad y causando colisiones entre los turismos, o saboteando los equipos que controlan el suministro de agua.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

A pesar de la trascendencia de la ciberseguridad para las entidades locales, y de la severidad de las amenazas planteadas en el escenario tecnológico, también es de reseñar la gravedad de los obstáculos que detectamos en este ámbito para afrontar dichos retos. Tales desafíos limitan su capacidad para proteger sistemas críticos, asegurar datos sensibles y garantizar la continuidad de los servicios públicos, además de suponer una relevante mengua en la protección de los derechos. Esquematizamos a continuación lo que hemos calificado de obstáculos:

– Limitaciones presupuestarias: Muchas entidades locales operan con recursos financieros restringidos en estas cuestiones, lo que dificulta la inversión en tecnología avanzada de ciberseguridad, personal especializado y formación adecuada. Los fondos disponibles suelen priorizar otros servicios, dejando la ciberseguridad en un segundo plano, lo que demuestra la poca altura de miras de algunos decisores locales.

– Falta de personal especializado: Todavía existe una escasez generalizada de profesionales capacitados en ciberseguridad, y las entidades locales tienen dificultades para atraer y retener talento, debido a salarios menos competitivos en comparación con el sector privado. Incluso, en muchos casos, el personal técnico local no tiene formación específica para enfrentar amenazas cibernéticas avanzadas. Es peligrosísimo que exista una brecha digital entre los *hackers* y ese personal técnico local.

– Infraestructuras tecnológicas obsoletas: Los sistemas informáticos en muchas entidades locales no están actualizados, y son más vulnerables a ataques cibernéticos. La dependencia de tecnologías antiguas complica la integración de soluciones modernas de seguridad. El empleo de *software* sin soporte o sistemas no actualizados es una puerta de entrada común para los atacantes.

– Falta de concienciación y formación: Tanto los funcionarios como los ciudadanos a menudo desconocen los riesgos asociados a la ciberseguridad, lo que aumenta la probabilidad de incidentes —como ataques de *phishing*— o del uso indebido de sistemas digitales. Un empleado que no identifica un correo de *phishing* o que reutiliza contraseñas débiles puede poner en riesgo toda la red. La formación en buenas prácticas de ciberseguridad no siempre se considera una prioridad, lo que otra vez evidencia lo ya dicho de falta de verdadero conocimiento de la gravedad de estos asuntos por parte de los decisores locales.

– Fragmentación y falta de cooperación: Las entidades locales a menudo trabajan de manera aislada, sin coordinarse con otras Administraciones

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

o agencias nacionales en temas de ciberseguridad. Esto limita el acceso a recursos compartidos, herramientas avanzadas y estrategias unificadas para enfrentar amenazas comunes.

– Pero al mismo tiempo que lo que acabamos de indicar, las entidades locales también suelen estar interconectadas con sistemas regionales o nacionales, lo que amplía la superficie de ataque. Un fallo en los sistemas de ciberseguridad de la Administración local puede tener consecuencias en cascada, afectando a otros organismos y servicios interconectados.

– Aumento en la sofisticación de las amenazas: Los ciberdelincuentes utilizan técnicas cada vez más complejas, como *ransomware* y ataques dirigidos, que son difíciles de prevenir y gestionar con los recursos locales limitados. Es decir, la sofisticación de las amenazas hace más peligrosos los déficits locales en ciberseguridad.

– Normativas complejas y en constante cambio: Las regulaciones de ciberseguridad, como el Reglamento UE 2016/679, de protección de datos, o la Directiva 2022/2555 (la NIS 2) en Europa, imponen obligaciones adicionales que las entidades locales pueden tener dificultades para cumplir, debido a su falta de capacidad técnica y financiera. Las normas europeas se han convertido habitualmente en muy complejas y abigarradas, lo que complica su aplicación. Las entidades locales deben cumplir con tales normativas de protección de datos y seguridad. Sin embargo, la falta de recursos y personal cualificado puede hacer que el cumplimiento sea difícil de garantizar.

Por lo tanto, como se ve, existen obstáculos relevantes que generan verdaderas dificultades para lograr una respuesta adecuada al desafío tecnológico, y que reclaman una concienciación rotunda por parte de los dirigentes locales.

6. ¿Qué deben hacer las entidades locales?

Visto todo lo anterior, se hace necesario que nuestro hilo argumental se centre ahora en la concreta respuesta que consideramos debe articular una entidad local, partiendo de esa lógica que impone la garantía de los derechos de las personas y la necesidad de que los servicios que se prestan tengan continuidad. En este sentido, las acciones para implementar deben ser diversas, algunas de calado, pero en todo caso articuladas de manera coordinada y coherente con ese fin último de garantía de los de-

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

rechos y mantenimiento de los servicios municipales, que tienen que ser la referencia permanente en estas actuaciones.

El punto de partida debe ser un **enfoque estratégico** que combine tecnología, capacitación, normativa y cooperación. Es decir, un planteamiento inicial horizontal y ambicioso, que parta desde el rigor. Una verdadera política que sea permanente y que evidencie la relevancia del desafío tecnológico. El responsable primero de esta política tiene que ser alguien de alto nivel en el *staff* de la entidad local, capaz de imponer las decisiones que haya que tomar y que pueda actuar de forma ágil. La inmediatez de los ciberataques obliga a dotar de similares características al entramado que protege frente a ellos.

Crear una **cultura de seguridad** dentro de las Administraciones locales es fundamental para que todos los empleados sean conscientes de las amenazas cibernéticas y de las mejores prácticas para proteger los sistemas. De este modo, la ciberseguridad debe constituir una política local clave y una inversión continua (económica, personal y material), una política que trate de diseñar e implementar un sistema de gestión de riesgos de la información adaptado al municipio, lo que implica ese enfoque estratégico al que nos referimos. Así, la ciberseguridad, desde esta lógica estratégica, debe ser considerada como un proceso continuo de mejora que desarrolle las fases de planificación[15], ejecución e implementación[16], que continúe con el seguimiento y la auditoría de medidas y controles implementados, y prosiga con la incorporación de mejoras o de adaptaciones correctivas respecto a la fase anterior, o medidas preventivas respecto de los nuevos riesgos que puedan surgir[17]. La seguridad de los sistemas de información "deberá comprometer a todos los miembros de la organización" (art. 13 del Real Decreto 311/2022, que regula el Esquema Nacional de Seguridad).

15. Fase encargada de establecer la política, objetivos, procesos y procedimientos relativos a la gestión del riesgo y a la mejora de la seguridad de la información de la organización, para ofrecer resultados acordes con sus políticas y objetivos generales.

16. En esta fase, se trataría de implementar y gestionar el sistema de gestión de seguridad de la información de acuerdo con su política, controles, procesos y procedimientos.

17. Pensemos que, si disponemos de copias de seguridad actualizadas y sufrimos un ataque de *ransomware*, el tiempo durante el cual dejemos de prestar los servicios será menor, al poder restaurarlos desde las copias. Una correcta segmentación de redes en los ayuntamientos ayudará en la contención de estos ataques, afectando solo a parte de los servicios municipales. De igual forma, frente a ataques de denegación de servicio, se preverá la instalación de sistemas distribuidos con balanceo de cargas, y se tendrá en cuenta el monitoreo de redes, de manera que los sistemas de detección y respuesta automatizada identifiquen y bloqueen el tráfico ante intentos de acceso no autorizados o sospechosos.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

A partir de esta política general de ciberseguridad, se deben aplicar un conjunto de acciones ya más específicas, entre las cuales destacamos las siguientes, que casi podemos considerar como imprescindibles ante el tamaño desafío que existe:

– La **evaluación de riesgos** y vulnerabilidades requiere efectuar auditorías regulares de ciberseguridad para identificar debilidades en sistemas y procesos. Se trata de adoptar un planteamiento de planificación proactivo, que se anticipe a los problemas que puedan surgir y se prepare ante las futuras contingencias. Esta política preventiva es la más aconsejable en el volátil y peligroso escenario tecnológico que nos envuelve, además de ser una exigencia del citado Esquema Nacional de Seguridad y de la normativa de protección de datos, ambos aplicables a las entidades locales.

  Así, el análisis de riesgos en protección de datos se deriva del principio de responsabilidad proactiva, considerándose obligatorio partir de dicha inferencia (art. 5 Reglamento UE 2016/679). A su vez, recordemos que el Esquema Nacional de Seguridad es en España un marco normativo establecido actualmente por el Decreto 311/2022, de 3 de mayo, que tiene como objetivo garantizar la protección adecuada de la información, los sistemas y los servicios electrónicos utilizados por las Administraciones públicas, lo que también incluye las entidades locales. De esta forma, se establecen medidas y principios para asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los datos que manejan los organismos públicos. La gestión de la seguridad basada en los riesgos es uno de los principios básicos de dicho Esquema Nacional de Seguridad, lo que significa que las medidas de seguridad se deben adaptar al nivel de riesgo que supone la información o el servicio.

– A partir de esta evaluación de riesgos, hay que desarrollar **políticas internas** claras sobre el uso de sistemas informáticos y la gestión de datos. En este sentido, deben elaborarse planes de contingencia y resiliencia que incluyan protocolos para responder a incidentes cibernéticos. Con dichos planes hay que asegurar la respuesta adecuada al hipotético ciberataque y la continuidad de los servicios. En este orden de cosas, también se puede aludir al diseño e implementación de soluciones tecnológicas específicas, como plataformas digitales para mejorar la participación ciudadana, sistemas de gestión de residuos inteligentes o redes de movilidad urbana conectadas. Sin una planificación adecuada, los ciberataques pueden paralizar servicios clave y afectar gravemente a los ciudadanos.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

– Es recomendable **categorizar** los distintos sistemas y procesos para priorizar aquellos más relevantes por razones objetivas, como el suministro de agua y electricidad o las bases de datos sensibles. Por ello, hay que priorizar la modernización de infraestructuras y áreas críticas mediante soluciones escalables y sostenibles.

– Resultan imprescindibles **buenas prácticas** de seguridad, como mantener *software* y sistemas operativos actualizados con los últimos parches de seguridad, o encriptar datos sensibles tanto en tránsito como en reposo, para prevenir accesos no autorizados. Las buenas prácticas mitigan en grado sumo el riesgo de los ataques.

– Hoy en día resulta inexcusable una **infraestructura tecnológica** robusta, asentada en unos estándares avanzados de seguridad y en herramientas de monitoreo constante. Se deben implementar medidas de protección tecnológica, herramientas que eviten la actuación del *malware* de los ciberataques. Así, deben emplearse *firewalls*, antivirus avanzados, sistemas de detección de intrusos, o herramientas de monitoreo en tiempo real. De igual forma, deben contemplarse sistemas de respaldo (*backups*) regulares para restaurar datos en caso de ataques. Y también sistemas de alerta temprana: sensores conectados para detectar anomalías, por ejemplo, en sistemas de suministro de agua o energía, protegidos contra ciberataques. Una aplicación de este tipo puede reportar los problemas municipales en tiempo real. Igualmente, las Administraciones locales deben garantizar que los servicios en la nube que contratan cumplan con los estándares de seguridad adecuados y ofrezcan protección contra vulnerabilidades.

  Pero no solo hay que poseer y reclamar los instrumentos tecnológicos oportunos, sino que también debemos tenerlos actualizados para que no se conviertan en un problema adicional. La actualización tecnológica es a veces una asignatura pendiente en los órganos públicos. Las entidades locales deben estar preparadas para realizar auditorías de seguridad y responder ante incidentes de manera rápida y efectiva, lo cual es un reto sin una estructura sólida de ciberseguridad.

– Como complemento de lo anterior deben realizarse **simulaciones** y pruebas de continuidad. Las simulaciones de ciberataques sirven para evaluar la capacidad de respuesta y la eficacia real de los protocolos de recuperación.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

– Sumamente útil resulta contar con un **plan de comunicación** para el tratamiento informativo de un ciberataque, en el que se debe buscar un equilibrio entre la adecuada transparencia de un poder público democrático y la necesidad de no mostrar una debilidad que atraiga más ataques. En nuestro mundo, la comunicación y la información se han vuelto imprescindibles en cualquier entramado organizacional y social. Un tratamiento correcto de estos extremos reporta estabilidad, credibilidad, confianza y, por ende, fortaleza. Los déficits en este campo son una verdadera debilidad, sobre todo en lo que concierne a la ciberseguridad.

– Hay que tener presente que el principal elemento de riesgo de ciberseguridad en una organización son sus empleados, que con su falta de **concienciación** en estos temas se convierten de forma involuntaria en una verdadera amenaza. Son los que no saben identificar un correo *phishing*, abren y pinchan en los enlaces sospechosos o intercambian datos de modo irreflexivo. Por ello, resulta fundamental **capacitar** al personal mediante una formación continua sobre buenas prácticas de ciberseguridad, en la que conozcan la realidad de los posibles ataques y de los medios de defensa, y logren estar concienciados y sensibilizados respecto de esta problemática. Así adoptarán siempre una actitud de cautela y precaución, y podrán identificar las amenazas comunes. Esta capacitación continua debe aplicarse a todo el personal, aunque más intensamente al personal técnico y administrativo y a los cuadros directivos.

– También puede ayudar de forma poderosa tener personas en el entramado administrativo con **especialización y responsabilidad específica** en estos ámbitos. El primero de ellos es el delegado de protección de datos (exigido para las entidades locales por el art. 37.1.a del citado Reglamento UE 2016/679). Este delegado debe ocupar un lugar clave en la política de ciberseguridad. Con sus funciones de asesoramiento y supervisión desempeña ese relevante rol.

  Pero, de igual forma, se puede designar a un encargado específico de ciberseguridad o a un equipo especializado en la gestión de riesgos digitales, que, en todo caso, deben estar coordinados con el delegado de protección de datos, evitando cualquier tipo de desajuste. Los desajustes internos favorecerán el éxito de los ciberataques y frustrarán o ralentizarán las respuestas.

  En este sentido, recordemos que el citado Real Decreto 311/2022, que regula el Esquema Nacional de Seguridad, en su art. 11.1 diferencia cuatro responsabilidades: “En los sistemas de información se diferenciará el res-

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

ponsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema". La política de seguridad de la entidad municipal "detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos" (art. 11.3)[18].

– Al margen de la dimensión interna de la Administración municipal, citamos igualmente en este apartado la actuación de cara al exterior, que también resultará útil en el propósito de incrementar la ciberseguridad. Así, las entidades locales deben **educar** a los ciudadanos sobre los riesgos cibernéticos, y promover su concienciación. En particular, hay que instruirlos en cómo proteger sus datos al interactuar con servicios digitales locales. A mayores, una opción interesante también es realizar campañas informativas sobre la importancia de contraseñas seguras y la verificación de identidad.

  Lo que debemos buscar es generar, a partir de varias iniciativas, una cultura de seguridad ciudadana. No cabe duda de que el fomento de la educación digital es la verdadera clave para conseguir una sociedad más protegida y vigilante ante los riesgos y amenazas del entorno tecnológico.

– El fomento de la **colaboración interinstitucional** es otro elemento útil que a veces no se contempla desde la óptica de la ciberseguridad. Conviene establecer redes de cooperación y apoyo mutuo con otras entidades locales, regionales y nacionales, para compartir información sobre amenazas y mejores prácticas. Incluso, en este sentido, podría resultar sugerente participar en programas o redes de ciberseguridad organizados por agencias estatales o internacionales. Recordemos que en España hay entidades que pueden colaborar, como el INCIBE o el Centro Criptológico Nacional. La necesaria interconexión exige una mayor coordinación y compartición de información sobre ciberamenazas con otros niveles de gobierno, lo que será complicado de gestionar sin las herramientas adecuadas. La cooperación interinstitucional es clave para mejorar las defensas y coordinar respuestas frente a incidentes.

18. El art. 13 de dicho decreto separa las cuatro funciones: "a) El responsable de la información determinará los requisitos de la información tratada b) El responsable del servicio determinará los requisitos de los servicios prestados. c) El responsable de la seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones. d) El responsable del sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad". El responsable de seguridad será en principio distinto al responsable del sistema.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

– De igual modo, gracias a su autonomía, los Gobiernos locales pueden establecer alianzas estratégicas con **empresas tecnológicas** para abordar problemas locales, como soluciones de eficiencia energética, proyectos de movilidad inteligente o desarrollo de aplicaciones de salud pública. En ello no deben comprometerse el servicio público ni la neutralidad propia de las entidades públicas.

– La **financiación** resulta clave para poder abordar esta problemática de manera robusta. Así, es fundamental aprovechar recursos externos y fondos públicos para modernizar infraestructuras y adoptar tecnologías avanzadas de ciberseguridad. En este sentido, pueden servir de referencia los estándares internacionales como la norma ISO/IEC 27001 para mejorar la gestión de la seguridad de la información. Asimismo, deben promoverse programas de financiamiento específicos para reforzar la ciberseguridad a nivel local, para lo cual se puede recurrir a fondos estatales y europeos.

– En línea de varias de las cosas comentadas, es imprescindible el **cumplimiento de la normativa**, tanto de protección de datos como más específica de ciberseguridad. Las entidades locales tienen que ser ejemplo del respeto al ordenamiento jurídico, en una época donde algunos relativizan estas cuestiones.

  En este sentido, en el derecho fundamental de **protección de datos**, la referencia es el tándem normativo que conforman el Reglamento UE 2016/679 y la Ley Orgánica 3/2018. Esta regulación ofrece un modelo proactivo para el tratamiento de los datos personales en el que el responsable del tratamiento asume la obligación de adoptar las medidas técnicas y organizativas adecuadas para respetar este derecho. En el ámbito local los responsables del tratamiento de datos suelen ser las personas jurídicas que suponen los ayuntamientos, diputaciones o cabildos. Se prevén una serie de principios que regirán este tratamiento, como el de transparencia, minimización, exactitud o confidencialidad; además, se contemplan derechos en manos de las personas interesadas que la entidad local debe cumplir (como los de acceso, rectificación, supresión, limitación, oposición o portabilidad) y obligaciones que pesan sobre estos órganos públicos (como las de información, realización de análisis de riesgos o evaluaciones de impacto, establecer un registro de actividades de tratamiento, nombrar al delegado de protección de datos, o formalizar el contrato con el encargado del tratamiento). El régimen sancionador en este sector normativo expone a la entidad local a sanciones si se producen violaciones de datos.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

– Hay que trabajar en **resiliencia** digital para mitigar las consecuencias negativas de un ciberataque. Así, debe contarse con redes municipales con copias de seguridad en la nube y procesos automáticos de restauración de datos tras un ataque.

– Aprovechando el progreso tecnológico, las entidades locales tienen que tratar de mejorar su funcionamiento democrático, lo que también podría ser útil en términos de ciberseguridad. De este modo, con mejores conocimientos en ciberseguridad, se puede apostar sin reticencias por vías tecnológicas que incrementen y dinamicen la **participación ciudadana**, esencia del propio concepto de democracia. Se trata de cuestiones relacionadas recíprocamente, pues una ciudadanía alfabetizada digitalmente puede usar mejor y sin temor esas nuevas opciones de participación, y tales nuevas opciones entrenan en parte a la ciudadanía en las habilidades tecnológicas. Así, las entidades locales pueden promover plataformas digitales que refuercen la participación activa de los ciudadanos, como consultas populares *online*, presupuestos participativos o mecanismos de transparencia en la gestión pública.

– En el mismo orden de cosas, los órganos locales deben esforzarse en la reducción de la **brecha digital** y en la subsiguiente inclusión digital, una cuestión básica en el moderno entendimiento del Estado social. En una comunidad local puede haber desigualdades injustificadas respecto al acceso a la tecnología, sea por razón de edad, capacidad económica o ubicación en el territorio del municipio. El Gobierno local tiene la obligación de afrontar estas desigualdades, que muchas veces se convierten en discriminación, y tratar de revertir la situación. Esto también incidirá de manera positiva en el incremento de los niveles de ciberseguridad.

Por lo tanto, son muchas las tareas que deben llevar a cabo las entidades locales en lo que ahora nos ocupa, la mayor parte de ellas necesarias en este momento de enorme penetración de la tecnología en la ciudadanía y en las distintas entidades privadas y públicas.

7. Conclusiones

Las entidades locales del presente y del futuro enfrentan importantes retos de ciberseguridad debido a la creciente digitalización de sus servicios, la limitada capacidad de recursos, la diversidad de datos que gestionan y el aumento de los ciberataques. La ciberseguridad no solo protege los derechos fundamentales de las personas, sino que también garantiza la información y los sistemas digitales de las entidades locales y asegura la

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

continuidad de servicios esenciales para la comunidad. Invertir en protección digital y establecer protocolos sólidos en la planificación y recuperación resultan esenciales para mantener la confianza pública y garantizar el bienestar local en un entorno tecnológico en constante evolución. El futuro incierto de esta evolución es un poderoso argumento adicional para reclamar esta constante y atenta atención que debe mostrarse en el ámbito local con la ciberseguridad. Tal atención tiene que basarse en una serie de ejes clave, como la defensa de la privacidad de las personas, la garantía de sus datos, y la efectividad de la participación ciudadana, que en buena medida depende de tener satisfechas sus exigencias de privacidad.

Se trata de una problemática de creciente complejidad, que en el futuro inmediato se hará más delicada y trascendente. Enfrentar estos desafíos requiere un enfoque estratégico, con apoyo financiero, formación adecuada y una coordinación efectiva entre los niveles de gobierno y la sociedad. Solo así podremos asegurar que las entidades locales estén mejor preparadas para proteger sus sistemas y garantizar la seguridad digital de su ciudadanía. Existen dos argumentos poderosos para obligar a la Administración local a prestar especial atención a la ciberseguridad, incluso para convertirla en un actor clave en ese sentido. Por un lado, la necesaria garantía de los derechos fundamentales, ahora ligados al mundo digital; y, por otro, lo imprescindible que resulta asegurar la continuidad de las funciones y los servicios, en la actualidad con habitual soporte tecnológico.

En Europa encontramos ya buenos ejemplos de trabajo municipal adecuado en términos de ciberseguridad, además de la implementación de distintos servicios y políticas que apuestan por la digitalización de forma segura. Un caso relevante son las plataformas de *smart cities* en municipios europeos, donde la autonomía local ha permitido la instalación de sensores en tiempo real para monitorizar el tráfico, mejorar el transporte, controlar la calidad del aire y mejorar la eficiencia energética y la recogida de residuos. Estas soluciones tecnológicas son posibles gracias a la flexibilidad y a la capacidad de decisión que proporciona la autonomía local. La digitalización correcta de servicios municipales debe traducirse en portales en línea para pagar impuestos, solicitar licencias o registrar quejas ciudadanas, que en todo caso aseguran la confidencialidad y la integridad de la información.

Desde la lógica de un análisis DAFO, la existencia de autonomía local es una verdadera oportunidad para tener éxito en ese esfuerzo. La autonomía local es un pilar fundamental para que las entidades locales enfrenten correctamente los desafíos tecnológicos, promoviendo respues-

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

tas innovadoras, eficaces y orientadas al bienestar de la ciudadanía. Esto asegura un entorno digital más seguro para la Administración y la ciudadanía. Ciertas características de las entidades locales también se configuran como una fortaleza. Es lo que sucede con la flexibilidad que podemos conseguir en la Administración local. La capacidad de adaptación de las entidades locales al desafío tecnológico depende de su flexibilidad, cercanía con los ciudadanos e inversión en recursos tecnológicos y humanos. Estas características las posicionan como actores fundamentales en la transformación digital de las comunidades, mejorando tanto la calidad de vida como la participación democrática en el entorno digital.

Sin embargo, la financiación puede ser una amenaza o una fortaleza en función de si resulta suficiente y adecuada o no. No cabe duda de que la financiación propia es clave para que las entidades locales puedan garantizar derechos fundamentales y desarrollar medidas eficaces de ciberseguridad. Este recurso otorga independencia, flexibilidad y capacidad para adaptarse a las necesidades locales, promoviendo un entorno más seguro y equitativo para la ciudadanía. Por tanto, las entidades locales deben esforzarse para conseguir los niveles de financiación que se necesitan.

En fin, la ciberseguridad como garantía de los derechos en el ámbito local repercute de manera directa en la confianza pública y participación ciudadana. Un entorno digital seguro fomenta la confianza de los ciudadanos en el uso de servicios en línea, como pagos electrónicos, consultas digitales y participación en presupuestos participativos. Esta ciberseguridad ya es la base imprescindible para la aplicación de las vías y los instrumentos de participación ciudadana, verdadera clave de un sistema democrático que controla efectivamente al poder. Esperemos que nuestras entidades locales puedan asumir todos estos retos y sean capaces de tener éxito en su marcha por el creciente mundo tecnológico.

8. Bibliografía

Álvarez Robles, T. (2018). Derechos digitales: especial interés en los derechos de acceso a internet y a la ciberseguridad como derechos constitucionales sustantivos. En A. I. Dueñas Castrillo, D. Fernández Cañueto y G. Moreno González (coords.). *Juventud y Constitución. Un estudio de la Constitución Española por los jóvenes en su cuarenta aniversario* (pp. 135-158). Zaragoza: Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico.

Álvarez Robles, T. (2024a). La ciberseguridad: la seguridad integral y descentralizada del Estado digital. En F. Caamaño y D. Jove Villares (dirs.). *Tecnologías abusivas y derecho* (pp. 255-293). Valencia: Tirant lo Blanch.

Álvarez Robles, T. (2024b). *El derecho de acceso a Internet: especial referencia al constitucionalismo español*. Valencia: Tirant lo Blanch.

Fernández Rodríguez, J. J. (2018). Ciberseguridad: ¿desafío insuperable? En búsqueda de escenarios de respuesta adecuados. En C. García Novoa y D. Santiago Iglesias (dirs.). *4ª Revolución Industrial: impacto de la automatización y la Inteligencia artificial en la sociedad y en la economía digital* (pp. 51-80). Cizur Menor: Aranzadi.

Fernández Rodríguez, J. J. (2020). Derechos y progreso tecnológico: pasado, presente y futuro. En W. Engelmann (coord.). *Sistema do direito, novas tecnologias, globalização e o constitucionalismo contemporâneo: desafios e perspectivas* (pp. 259-277). São Leopolodo: Casa Leiria.

Fernández Rodríguez, J. J. (2023). Reflexiones (provisionales) sobre los derechos de los robots. En M. A. Rocha Espíndola, D. Sansó-Rubert Pascual y N. Rodríguez Dos Santos (coords.). *Inteligencia artificial y derecho. Reflexiones jurídicas para el debate sobre su desarrollo y aplicación* (pp. 227-242). Madrid: Dykinson.

Fernández Rodríguez, J. J. (2024). *¿La manipulación informativa destruirá a la democracia?* A Coruña: Colex.

Fernández Rodríguez, J. J. e Iglesias Barral, S. (2012). Gobierno electrónico: posibilidades en el ámbito judicial. *Revista Mexicana de Análisis Político y Administración Pública*, 1 (2), 73-93.

Greiff, G. (2005). Terrorismo y seguridad nacional. El derecho internacional que hereda el siglo XXI. En R. Méndez Silva (coord.). *Derecho y seguridad internacional. Memoria del Congreso Internacional de Culturas y Sistemas Jurídicos Comparados* (pp. 137-159). Ciudad de México: UNAM.

Hobbes, T. (1651). *El Leviatán*. Londres: Andrew Crooke.

Pérez Royo, J. (2010). La democracia frente al terrorismo global. En J. Pérez Royo y M. Carrasco Durán (dirs.). *Terrorismo, democracia y seguridad, en perspectiva constitucional* (pp. 7-12). Barcelona: Marcial Pons.

Rebollo Puig, M. (2019). La trama de la Ley de Seguridad Ciudadana. En M. Izquierdo Carrasco y L. Alarcón Sotomayor (dirs.). *Estudios sobre la Ley Orgánica de Seguridad Ciudadana* (pp. 31-170). Pamplona: Aranzadi.

Ridaura Martínez, M.ª J. (2014). La seguridad ciudadana como función del Estado. Estudios de Deusto, 62 (2), 319-346.

Rodríguez, R. J. (2023). *A brief history of malware* (part 1). Blog Rme-Disco Research Group, 28 de febrero de 2023. Disponible en https://reversea.me/index.php/a-brief-history-of-malware-part-1/.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6