## JORNADA “INTELIGENCIA ARTIFICIAL Y GOBIERNOS LOCALES”

**SEVILLA, 23 de marzo de 2022**

# CIBERSEGURIDAD Y GOBIERNOS LOCALES

**Dra. Dolors CANALS AMETLLER**
Profesora Titular de Derecho Administrativo
Facultad de Derecho - Universitat de Girona
dolors.canals@udg.edu

Universitat de Girona
**Departament de Dret Públic**

# I. LOS GOBIERNOS LOCALES EN LA "SOCIEDAD DEL RIESGO DIGITAL"

- De la "**sociedad del riesgo**" (Ulrich Beck: 1986) a la "**SOCIEDAD DEL RIESGO DIGITAL: "hibridación de riesgos y amenazas": INVERTIR EN CIBERSERGURIDAD ES UN ACTIVO**

- **CORRESPONSABILIDAD PÚBLICO-PRIVADA E INDIVIDUAL en materia de seguridad digital: SEGURIDAD DIGITAL COLECTIVA Y COLABORATIVA**

- **CONCIENCIA y CULTURA de la ciberseguridad**": "***auto-seguridad* digital" vs. "seguridad pública digital"**

- "**FORMACIÓN en competencias digitales y en ciberseguridad**" ("**función pública digital/teletrabajo**"): incluye formación en "protección de datos personales/empresariales": "***información digital sensible***": **DATOS como bienes a proteger y como objeto de mercado y "materia prima de la producción digital": Inteligencia Artificial: en el CIBERESPACIO somos DATOS: art. 83 LOPDCP: seguridad de las comunicaciones en la Red**

- **TRANSFORMACIÓN/TRANSICIÓN DIGITAL de las AAPP/EELL: mayor digitalización significa mayor inseguridad ("LO *INTELIGENTE* ES INSEGURO")**

# II. CONCEPTOS CLAVE Y PANORÁMICA

**CIBERSEGURIDAD: STC Sentencia 142/2018, de 20 de diciembre de 2018 :**

**FJ 4**: "La **Unión Internacional de Telecomunicaciones** define la ciberseguridad como el «**conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno**» (Recomendación de la Unión Internacional de Telecomunicaciones UIT-T X.1205). Por su parte, en **la Directiva (UE) 2016/1148, de 6 de julio, del Parlamento Europeo y del Consejo, se define la «seguridad de las redes y sistemas de información» como «la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información accesibles a través de ellos»** (art. 4.2). Con esta finalidad, y según la propia Directiva, los Estados pueden adoptar medidas de **«prevención, detección, respuesta y mitigación de los incidentes y riesgos que afecten a las redes y sistemas de información»** (considerando 34).

Dado el contenido de los diversos aspectos que configuran el **concepto de la ciberseguridad**, es posible considerar que ésta puede tener **varias acepciones y comprender varias actividades**. (…) En lo que a efectos del presente proceso interesa, hay que mencionar, en primer lugar, **la relacionada con la adopción de medidas ordinarias de prevención o seguridad de la red y, en general, de las tecnologías de la información**. En particular, **respecto a la ADMINISTRACIÓN ELECTRÓNICA, garantizando la protección de las redes de comunicaciones electrónicas que esta genere y la protección de los derechos de los administrados en sus relaciones con las administraciones públicas a través de medios electrónicos.** No discute el Abogado del Estado, que las **Comunidades Autónomas** pueden, al amparo de las competencias que sus Estatutos de Autonomía les reconocen, **adoptar determinadas medidas dirigidas a garantizar la protección de sus infraestructuras y la seguridad de las tecnologías de la información y la comunicación**. Medidas en este ámbito que, en muchas ocasiones, vienen reclamadas por las propias normas estatales (así, por ejemplo, el Real Decreto 3/2010, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad en el ámbito de la Administración electrónica** ….)".

# II. CONCEPTOS CLAVE Y PANORÁMICA

FJ 4: "La **ciberseguridad, como sinónimo de la seguridad en la red, es una actividad que se integra en la seguridad pública, así como en las telecomunicaciones. A partir de su conceptuación como conjunto de mecanismos dirigidos a la protección de las infraestructuras informáticas y de la información digital que albergan, fácilmente se infiere que, en tanto que dedicada a la seguridad de las tecnologías de la información, presenta un componente tuitivo que se proyecta específicamente sobre el concreto ámbito de la protección de las redes y sistemas de información que utilizan los ciudadanos, empresas y administraciones públicas**. El uso cotidiano de las tecnologías de la información y la comunicación ha provocado que se conviertan en un elemento esencial para el desarrollo económico y las relaciones sociales. No obstante, es también un hecho constatado que las amenazas a la seguridad de la red comportan un riesgo que afecta a los ámbitos más diversos, por cuanto pueden afectar a la disponibilidad, integridad y confidencialidad de la información". ("Seguridad de la información")

"En el ATC 29/2018, de 20 de marzo, FJ 5, ya se constató **la conexión existente entre ciberseguridad y seguridad nacional «incluida como dice expresamente la Ley 36/2015, en los títulos competenciales de las materias 4 y 29 del artículo 149.1 CE»** (STC 184/2016, FJ 3), pues **la Ley 36/2015, de 28 de septiembre, de SEGURIDAD NACIONAL, identifica en su artículo 10 la ciberseguridad como uno de los «ámbitos de especial interés de la seguridad nacional... que requieren una atención específica, por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales**». También la **Ley 8/2011, de 28 abril, de medidas para la protección de las INFRAESTRUCTURAS CRITICAS, dictada al amparo de la competencia atribuida al Estado en virtud del artículo 149.1.29 CE, hace referencia a la ciberseguridad**". "…. Tales **SERVICIOS ESENCIALES son los necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las Administraciones públicas (…)":**

**AAPP INTERCONNECTADAS E INTEROPERABLES: INCREMENTO Y EXTENSIÓN DE RIESGOS DIGITALES**

**DIGITALIZACIÓN DE SERVICIOS PÚBLICOS: SEGURIDAD EN LOS SERVICIOS DIGITALES (e infraestructuras)**

# II. CONCEPTOS CLAVE Y PANORÁMICA

## CIBERSEGURIDAD EN LAS ADMINISTRACIONES PÚBLICAS LOCALES:

No se trata exclusivamente de la seguridad informática; también de la **seguridad corporativa y ciudadana**, y, con ello, de **UNA POLITICA PUBLICA DE SEGURIDAD DIGITAL** que garantice, de forma razonable y suficiente la seguridad frente a las amenazas procedentes del ciberespacio.

La transformación digital de los municipios, con independencia de su dimensión institucional, poblacional y/o territorial, les obliga a garantizar la seguridad de los ciudadanos que se relacionan con ellos por medios electrónicos y digitales. Esta nueva **obligación** parece entenderse como **una función inherente a los servicios de administración electrónica, cuya ineficiente gestión podría generar incluso una eventual responsabilidad patrimonial en caso de daños**. Este **nuevo deber jurídico** abarca tanto la organización de medios y la previsión de medidas de protección de la organización administrativa como de los derechos de la ciudadanía.

El **Plan de Recuperación, Transformación y Resiliencia de la economía española (PRTR), aprobado por la Comisión Europea el 16 de junio de 2021**, con el objetivo de recuperar nuestra economía tras la crisis sanitaria, se incluye la **Componente 15 del PRTR "Conectividad digital, impulso de la ciberseguridad y despliegue del 5G**", que prevé la aprobación de una nueva ley general de telecomunicaciones, transposición interna de la Directiva 2018/1972 del Código Europeo de Comunicaciones Electrónicas: **"LO QUE ESTÁ POR VENIR…"**

# II. CONCEPTOS CLAVE Y PANORÁMICA

- **Gestión de la seguridad digital y REPARTO COMPETENCIAL Estado-CCAA-EELL en materia de uso de medios electrónicos por las administraciones públicas y garantía de la ciberseguridad**: POTESTADES, COMPETENCIAS, SERVIVICOS Y OBLIGACIONES LEGALES ¿Hablamos de lo mismo?

  - La **CE NO INCLUYE ningún reparto de competencias en materia de medios electrónicos, de digitalización o de gestión administrativa electrónica más allá del art. 149.1.18ª** (bases del régimen jurídico de las Administraciones públicas y del régimen estatutario de sus funcionarios que, en todo caso, garantizarán a los administrados un tratamiento común ante ellas; el procedimiento administrativo común, sin perjuicio de las especialidades derivadas de la organización propia de las Comunidades Autónomas…). Pero, **CIBERSEGURIDAD arrastra la competencia estatal ex art. 149.1.21ª (competencia en telecomunicaciones) y 29ª (competencia en seguridad pública y al margen la seguridad nacional: ¿título extensible?)**

  - **Real Decreto 203/2021, de 30 de marzo** (el Reglamento de actuación y funcionamiento del sector público por medios electrónicos): **modifica el Real Decreto 931/2017, de 27 de octubre**, para incorporar en la Memoria del Análisis de Impacto Normativo (**MAIN procesos normativos AGE**) "el análisis de la ***incidencia en los gastos en medios o servicios de la Administración digital dentro del impacto presupuestario de los proyectos*** y, por otra parte, para ***incluir dentro del apartado de «Otros impactos»*** *el que tendrá para* ***las personas destinatarias de la norma y para la organización y funcionamiento de la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la aplicación de la normativa proyectada": SIN MENCIÓN ALGUNA A LA DESIGUALDAD MUNICIPAL existente*** **("pensar a pequeña escala")**

  - **Ley de Bases de Régimen Local** (LRBRL modificación LRSAL): **DIPUTACIONES PROVINCIALES: atribución de "NUEVAS" competencias en prestación de servicios de administración electrónica y contratación en los municipios de menos de 20.000 habitantes ("INSTRUMENTALIZACION DE LAS DIPUTACIONES PROVINCIALES para el CUMPLIMIENTO NORMATIVO de las entidades municipales"): ¿también en garantía de la seguridad digital? La "ADMINISTRACION DIGITAL y AUTOMATIZADA" no es lo mismo que la "ADMINISTRACIÓN ELECTRÓNICA": ¿Existen "otras soluciones de gestión" posibles?**

# III. MARCO NORMATIVO Y DE ESTANDARIZACIÓN TÉCNICO-JURÍDICA

- **Leyes 39/215 y 40/2015 (en lo básico): Transmisiones de datos entre Administraciones Públicas) y ENS**
- **Ley Orgánica 2/2018 de Protección de Datos (OBLIGACIONES LEGALES y NUEVOS SUJETOS: delegado y responsable de datos): RÉGIMEN SANCIONADOR para las AAPP (art. 77) y OBLIGACIONES EXTENDIDAS A LOS CONTRATISTAS, tb el ENS: LEGISLACION DE CONTRATACION PUBLICA (disp. ad. 25)**
- **Real Decreto 203/2021, de 30 de marzo: Reglamento de actuación y funcionamiento del sector público por medios electrónicos (en lo básico)**
  - **CIBERSEGURIDAD**: arts.15 (sistemas de identificación, firma y verificación), 16 (plataformas de verificación de certificados electrónicos y de otros sistemas de identificación), 23 (certificados electrónicos de empleado público con número de identificación profesional), 26 (sistemas de identificación de las personas interesadas en el procedimiento), 28.2 y 3 (sistemas de clave concertada), 29.4 (autorización previa del Mº de Transformación Digital de sistemas de firma electrónica) y disposición adicional tercera (Nodo de interoperabilidad de identificación electrónica del Reino de España).
- **Real Decreto 3/2010, de 8 de enero, Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS: creado por Ley 11/2007), instrucciones y normas de desarrollo** (modificado en 2015)**: no es solo SEGURIDAD INFORMATICA, también es SEGURIDAD CORPORATIVA.**

  **ENS:** Define **PRINCIPIOS y REQUISITOS BÁSICOS para una POLITICA DE SEGURIDAD DIGITAL** en el uso de medios electrónicos por las AAPP que permita una **adecuada PROTECCION de la INFORMACION y DATOS** de una administración y **garantizar la SEGURIDAD de los SISTEMAS, los DATOS, las COMUNICACIONES y los SERVICIOS PÚBLICOS ELECTRÓNICOS**, cumpliendo con la normativa en materia de seguridad digital y protección de datos. **Con este objetivo, garantizar este cumplimiento normativo, se estandarizan o normalizan todas la las actuaciones y procedimientos a aplicar por el Centro Criptológico Nacional (CCN)**. Es un sistema que se basa en la **Declaración y Certificación de Conformidad con el ENS**, que obliga a un proceso independiente de auditoría a través de entidades acreditadas por la ENAC: emiten un certificado de conformidad que debe ser expuesto en las webs institucionales, y **en un proceso de análisis y gestión de riesgos y comunicación de INCIDENTES de SEGURIDAD**.

  **- Guía de Seguridad de las TIC CNN-STIC 883** (mayo de 2020): **Guía de implementación del ENS para EELL**
- **Real Decreto 4/2010, de 8 de marzo, Esquema Nacional de Interoperabilidad (ENI) en el ámbito de la administración electrónica y normas técnicas de desarrollo** (relacionadas en el Real Decreto 203/2021, de 30 de marzo, que lo modifica)
- **Real Decreto-Ley 12/2018 de seguridad de redes y sistemas de información, modificado por RD 43/2021: gestión y notificación de ciber-incidentes (servicios esenciales y servicios digitales) (tb para datos sensibles)**

# III. MARCO NORMATIVO Y DE ESTANDARIZACIÓN TÉCNICO-JURÍDICA

- **FEMP:**
  - Guía Estratégica en Seguridad para las Entidades Locales (ENS) (recomendaciones) (Tomo 1)
  - Guía para Entidades Locales de menos de 2.000 habitantes (recomendaciones) (Tomo 2): prevé la delegación de ciertas responsabilidades ("responsable de seguridad de sistemas de información") a la DIPUTACION PROVINCIAL

- **CCN Y FEMP: abril 2021: "Prontuario de ciberseguridad para las Entidades locales":** *"Los responsables locales deben encontrar FÓRMULAS INNOVADORAS de garantizar la sostenibilidad de tales servicios (digitales)"*

- ***Instrucciones técnicas (normas técnicas) y recomendaciones y GUIAS CCN-CERT: servicio de capacidad de respuesta a incidentes de seguridad de la información del Centro Nacional Criptológico del CNI* (desde 2006)**
  ***OFRECE TAMBIEN HERRAMIENTAS INFORMATICAS DE PROTECCION DIRECTA contra infecciones por códigos dañinos ("SOLUCIONES")***
  ***Anualmente publica informes sobre agentes dañinos y recomendaciones***

- **FEMP: Orientaciones para la adaptación de las Administraciones locales al Reglamento General (UE) de Protección de Datos**

- **AEPD: Guía sectorial "Protección de Datos y Administración local":** responsables del tratamiento de datos lo son los Ayuntamientos y las Diputaciones provinciales serán responsables del tratamiento de datos derivados de la prestación de asistencia en favor de los municipios // **DELEGADO DE PROTECCIÓN DE DATOS** en los municipios de menos de 20.000 hab : delegado propio, a través de la Diputación provincial o la respectiva CCAA, o "entidades privadas especializadas"; y **SEGURIDAD del tratamiento de los datos**: el análisis de riesgo puede llevarse a cabo con el soporte de la Diputación provincial

- **AEPD: Guía para la notificación de brechas de datos personales**

- **LO QUE ESTA POR VENIR:** nueva identidad digital europea; proyecto de ley de seguridad nacional (se ha anunciado un anteproyecto de ley de ciberseguridad); proyecto de ley de telecomunicaciones; nueva directiva NIS2 (redes y sistemas de información: para garantizar un elevado nivel común de ciberseguridad en la UE: propuesta 2020) y nueva Directiva relativa a la resiliencia de las ENTIDADES CRITICAS (propuesta 2020) esto es, sectores e infraestructuras consideradas esenciales: ahora "entidades esenciales" y "entidades importantes" de acuerdo con la terminología europea

# IV. GOBERNANZA DE LA CIBERSEGURIDAD

- **UE: Agencia de la Unión Europea para la Ciberseguridad (ENISA)**

- **ESTADO:**

  - **CONSEJO DE SEGURIDAD NACIONAL (Presidencia del Gobierno)**
  - **MINISTERIO DE DEFENSA**
  - **MINISTERIO DE TRANSICIÓN DIGITAL**
  - **CENTRO NACIONAL DE INTELIGENCIA (CNI):** Ley 11/2002, de mayo, reguladora del CNI: garantizar la seguridad de las tecnologías de la información en el ámbito de las AAPP: a través del CCN:

    - **CENTRO CRIPTOGRAFICO NACIONAL (CCN): ORGANISMO CENTRAL REGULADOR Y GESTOR DE LA CIBERSEGURIDAD PÚBLICA**

- **Comunidades Autónomas: Agencia de Ciberseguridad de Catalunya y Normativa de ADMINISTRACION DIGITAL**

  - **Políticas de seguridad AUTONOMICAS (en base al ENS)**
  - **Políticas de seguridad MUNICIPALES (en base al ENS)**

- **Tribunal de Cuentas y OCEX (organismos de control externo**): fiscalización externa de cumplimiento de la legalidad en materia de ciberseguridad (normativa Esquena Nacional de Seguridad)

# V. GESTIÓN LOCAL COLABORATIVA

- **El rol de la DIPUTACIÓN PROVINCIAL:**
  - **LRBRL: DIPUTACIONES PROVINCIALES:** Competencias en prestación de servicios de administración electrónica y contratación en los municipios de menos de 20.000 habitantes: **¿incluye la implementación y gestión de la seguridad digital y protección de datos?**
  - **El rol de la DIPUTACIÓN PROVINCIAL: carácter asistencial respecto de los pequeños y medianos municipios: ¿delegación de "nuevas" responsabilidades?**

- **Concretas problemáticas y retos actuales (**Agenda 2030, Economía Circular, cambio climático, pandemias-salud, ciberseguridad) que afectan a las administraciones públicas, incluidas las municipales y locales, pero que**:**
  - **superan los límites territoriales en los que ejercen sus competencias**
  - **implican nuevas obligaciones de cumplimiento normativo y responsabilidades, que no son propiamente competencias** (ni "competencias propias" ni "competencias delegadas")
  - **comportan la necesidad de rectificar/modificar los criterios de atribución de competencias por el legislador estatal/autonómico**
  - **exigen mecanismos de colaboración entre administraciones públicas organizadas en RED: COLABORACIÓN EN RED (a través o no de la Red): colaboración en caso de INCIDENTE de SEGURIDAD y compartición de BUENAS PRÁCTICAS**
  - **exigen marcos jurídicos y arquitecturas de colaboración público-privado: la entidad del CONSORCIO LOCAL: GESTIÓN LOCAL COLABORATIVA**

**Descongestión competencial de las Diputaciones provinciales: apoderamiento competencial ante el avance de la administración electrónica y la seguridad digital:**

**Los consorcios locales ¿una solución alternativa?**

**Asociaciones municipales y agrupación para la contratación/compra compartida de servicios y programas informáticos**

**GESTION LOCAL COLABORATIVA EN REDES:** Superación de estructuras de gestión administrativa ordinaria y creación de estructuras de gestión colaborativa público-privada **EN RED**

CANALS AMETLLER, D. (Dir.) (2021), *Ciberseguridad. Un nuevo reto para el Estado y los Gobiernos Locales,* Wolters Kluwer: Madrid.

CANALS AMETLLER, D. (2022): “La seguridad digital en medianas y pequeñas entidades locales: hacia una gestión municipal colaborativa”, en *Transformación digital en las medianas y pequeñas entidades locales: retos en clave de eficiencia y sostenibilidad,* Wolters Kluwer: Madrid (EN PRENSA).

FEDERACIÓN ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS, Y CENTRO CRIPTOGRÁFICO NACIONAL, (2021), *Prontuario de ciberseguridad para las Entidades locales,* abril 2021.

FEDERACIÓN ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS (2018), *Guía Estratégica de Seguridad para Entidades Locales. Esquena Nacional de Seguridad (ENS). Cuaderno de Recomendaciones. Tomo 1*.

FEDERACIÓN ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS (2018), *Guía para Entidades Locales de menos de 20.000 habitantes. Esquena Nacional de Seguridad (ENS). Cuaderno de Recomendaciones Tomo 2.*

FONDEVILA ANTOLÍN, J, (2017), “Seguridad en la utilización de medios electrónicos. El Esquena Nacional de Seguridad”, en Gamero Casado, E. (Dir.): *Tratado de Procedimiento Administrativo Común y Régimen Jurídico Básico del Sector Público,* Tirant lo Blanch, Valencia, pp. 549 y ss.

FONDEVILA ANTOLÍN, J, (2017), “Administración electrónica y contratación pública: algunas consideraciones en materia de seguridad”, en Martín Delgado, I. (Dir.): *La reforma de la administración electrónica: una oportunidad para la innovación desde el derecho,* Instituto Nacional de Administración Pública (INAP): Madrid.

# GRACIAS!

Universitat de Girona
Departament de Dret Públic