DERECHO DE CIBERSEGURIDAD

La **legislación española** en este ámbito ha cambiado significativamente en los últimos años. Sin embargo, el Gobierno ha anunciado recientemente la **"España digital 2025"**, un plan que contiene 47 medidas (mayormente políticas) para impulsar la transformación digital en España.
El plan propone una reforma y una propuesta. La reforma es para la AP y la propuesta es para toda la población, el Gobierno no puede imponer su criterio. Hay buenas intenciones pero las limitaciones son amplias. En 2023 se modificarán de manera exponencial. Se quedarán de manera genérica.

- Tiene limitaciones evidentes (ej.: ciberataques Rusia han transformado los contenidos de los 47 puntos)
- Reactualización de medidas que ya estaban en camino
- Pero no se tiene en cuenta el mando de ciberdefensa, la inteligencia económica en el mundo digital
- Se mantiene el problema de la seguridad y solvencia
- No hay un soporte telefónico para que les pueda proveer de soluciones de información
- Va a ser modificado por completo por los ataques continuos

En cuanto a la **implementación de la Directiva NIS**, el Gobierno aprobó una **ley** (mediante la aprobación de un Decreto-Ley) aunque aún **NO** se ha probado un **reglamento** para desarrollar la ley.

Directiva UE 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

- **RD 12/2018**: regula la seguridad de las redes y los sistemas de información utilizados para la provisión de los servicios esenciales y los servicios digitales, estableciendo mecanismos que permiten mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información, y fijando un marco institucional de cooperación que facilita la coordinación de las actuaciones (nivel nacional y europeo).
- **RD 43/2021**: desarrolla el RD en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información al cumplimiento de las obligaciones de seguridad de los operadores de los servicios esenciales y de los proveedores de servicios digitales y a la gestión de incidentes de seguridad.

*Un borrador de norma sobre seguridad en la tecnología 5G también se encuentra en una etapa preliminar. El Gobierno ha llevado a cabo una consulta pública sobre su idoneidad).

Lo que se hace con esto es demorar de forma deliberada pero acusando a otras partes. Se hacen las famosas **consultas públicas** y con eso ganas **6 meses** (le contamos el cuento a Bruselas de que estamos con consulta pública). El Gobierno no quiere aplicarlo y lo intenta obstaculizar, demorar, …

FUNDAMENTOS JURÍDICOS

Sentencia TC 148/2000 01/06 (FJ 10): definición de **Seguridad Pública** como "*todas aquellas medidas o cautelas que, dirigiéndose a la protección de personas y bienes, tengan como finalidad aún más específica evitar graves riesgos potenciales de alternación del orden ciudadano y de la tranquilidad pública" (FJ 10).*

- A través de la necesaria puesta en práctica de medidas preventivas y reactivas íntimamente relacionadas.
- Es lo que opera normativamente en España

Sentencia TC 145/2005 09/06 (FJ 5)
La doble condicionalidad en Seguridad Pública: para la efectiva asunción competencial en materia de seguridad pública por parte de las CCAA, no basta con una previsión estatutaria, sino que la CE exige que se haga en el marco de lo que disponga una LO distinta. El TC ha considerado la creación de policías autonómicas como "habilitan de una asunción competencial en relación con los correspondientes servicios politíceles, pero también co ala actividad administrativa que le sea inseparable por razón de inherencia o complementariedad".

- **Ámbito material seguridad pública**: actividades policiales (seguridad pública en sentido amplio)

Delimitación **ámbito competencial CCAA**

1. Creación de **policía autonómica** (por LO y prevista en los Estatutos)
- Referencia orgánica: organización
- Referencia funcional: ejercicio únicamente dentro de su territorio de las funciones o servicios policiales no estatales.

2. Ámbito de la **actividad estrictamente policial**. Incluye: potestades administrativas (complementarias e inherentes) cuando no guarden relación alguna con la actividad policial estatal.

Han de incluirse en el ámbito competencial de las CCAA que dispongan de policía de seguridad propia todas aquellas facultades que, bien por su especifidad o bien por inherencia o complementariedad, sean propias de las funciones o servicios policiales que hayan asumido con arreglo a lo dispuesto en los respectivos estatutos y en la LOFFCCSS (Ley 2/1986).

Corresponden al **Estado**:
- Servicios policiales reservados
- Restantes potestades o facultades administrativas que, siendo relevantes para la seguridad pública, no sean propias ni inherentes de las funciones o servicios policiales.

*Las policías autonómicas pueden desplegarse como investigadores en casos de ciberdelitos, en mas situaciones que hasta ese momento se contemplaban.

Sentencia TC 31/2010 28/06 (FJ 109): respecto a la competencia sobre los "sistemas de videovigilancia", el Tribunal Constitucional estableció que cabe "admitir el control autonómico sobre empresas y establecimientos privados, sin perjuicio de que para asegurar la virtualidad de la competencia estatal sea necesaria la puesta en juego de los mecanismos de coordinación y cooperación" que pueden ser todo lo intensos que se estime conveniente para el logro del objetivo de la seguridad pública, cuya tutela corresponde al Estado (FJ 109).

Art. 173 EAC ¿vulnera la competencia exclusiva del Estado en materia de seguridad pública?

NO vulnera - Las técnicas del art. 173 EAC son técnicas instrumentales necesarias para la actuación de la policía autonómica. SOLO hay uso y control de sistemas de videovigilancia.

Reserva de LO del art. 81.1 CE cuando la videovigilancia afecta a DDFF.

El art. 173 RAC NO atribuye a la Generalitat competencia alguna sobre la regulación del uso de estas técnicas, sino **exclusivamente sobre el uso y control** que de estas génicas se hagan por parte de la policía autonómica o empresas de seguridad autorizadas.

Sentencia TC 142/2018 de 20 de diciembre de 2018

Definición de **ciberseguridad**: 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.

Directiva UE 2016/1148 "seguridad de las redes y sistemas de información"
Capacidad de las redes y sistemas de información de resistir con un nivel determinado de fiabilidad toda acciona que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidnos o tratados, o los servicios ofrecidos por tales redes y sistemas de información.

El **TC** asienta que la ciberseguridad se integra en las competencias estatales en materia de seguridad publica y telecomunicaciones, dado que se incluye en ámbitos competenciales estatales en cuanto al referirse a las necesarias acciones de prevención, detección y respuesta frente a las ciberamenazas, afecta a cuestiones relacionadas con la seguridad pública y la defensa, las infraestructuras, redes y sistemas y el régimen general de telecomunicaciones (FJ 4).

Las competencias autonómicas no permiten amparar una pretensión de configurar una garantía general y omnicomprensiva de ciberseguridad. Ni siquiera el estado lo puede hacer. El avance del delito es más rápido que el del estado protegiendo.

Sentencia TC 184/2016 de 3 de noviembre de 2016: acotación jurídica de Seguridad Nacional. El TC consolidó la primacía del estado, pues siendo clara la competencia estatal, tanto en materia de defensa como en materia de seguridad publica, no tendría sentido que en un amito como la seguridad nacional, tan estrechamente vinculado a ambas, hasta el punto de identificarse sus fines y objetivos y los bienes jurídicos protegidos en la forma indicada, la competencia estatal pasará a ser puramente residual. Por tanto, concluye el alto tribunal que la seguridad nacional "no es una competencia nueva sino que se integra en las competencias estatales de defensa y seguridad pública" (FJ 3).
Dentro de seguridad nacional hay una parte importante dedicada al espacio ciber, que debe ser protegido.

A este respecto, se recomiendan los relevantes Fundamentos Jurídicos 6 y 7 de la **STC 175/1999 de 30 de septiembre de 1999.** En particular, los meditados "mecanismos de coordinación y cooperación" pueden ser "todo lo intensos que se estimen convenientes para el logro del objetivo de la seguridad pública, cuya tutela correspondiente al Estado" **(FJ 6 y 7 MUY IMPORTANTES PREGUNTA EXAMEN).**

FJ 6: los sistemas de verificación y registro de establecimientos localizados en un ámbito territorial determinado —> competencia de la CCAA donde radiquen.

El objeto de la competencia sí es objeto de fraccionamientos y por lo tanto puede llevarse a cabo mediante mecanismos de cooperación y coordinación (no requiere grado de homogeneidad por parte del Estado).

FJ 7: para garantizar la seguridad pública en el conjunto del territorio nacional el Estado puede establecer mecanismos de cooperación y relativos a los sistemas de registro y control, en especial al traslado de la información derivada de los mismos.

Siempre primará la tutela del estado pero enorme flexibilidad a la hora de conseguir los objetivos de seguridad pública.

DOCTRINA DE DERECHO AL OLVIDO

- **Sentencias judiciales**: acotación de los límites del derecho al olvido
- **TS**: el derecho al olvido es un derecho **diferente** a los protegidos por las normas de protección de datos porque es un derecho cuya aplicación en algunos casos es del todo inasible (no se puede aplicar). Ej.: yo prohibo que salgan esas fotos, y al cabo de media hora salen 80 más ¿cómo controlas eso? Y cuanto más presionas para que no salga y más te expones, peor. Actitud prudente en muchas ocasiones: callarse.
- **Ley de Protección de Datos**: reconocimiento de un derecho digital al olvido

Hoy por hoy el derecho al olvido al 100% no existe, todo puede ser replicado. El mejor consejo: no dejar en internet aquello que no quieras que sea visto por otros. Hoy el problema es la necesidad de exhibicionismo.

- **Sentencia TS de 11 de enero de 2019**: impone necesidad de sopesar circunstancias tales como la "veracidad de la noticia o enlace, la proyección pública del personaje".

- **Sentencia TEDH de 18 de septiembre de 2014**: requirió la ponderación del factor tiempo, así como su pertinencia y proporción, ante la posibilidad del ejercicio del derecho al olvido.

- **SENTENCIA TJUE DE 24 DE SEPTIEMBRE DE 2019**: se delimita el **alcance del derecho al olvido**. ***MUY IMPORTANTE. ESTUDIAR PARA EL DÍA DEL EXAMEN**

Google vs Comisión nacional de informática y libertades

*Decisión prejudicial —> interpretación Directiva UE 95/46/CE (1995)

CNIL impone sanción de 100.000€ por negarse a retirar los enlaces de una lista de resultados en todas las extensiones de nombre de dominio de su motor de búsqueda.

Reglamento UE 2016/679 - deroga Directiva

- Es de aplicación ya que aunque Google no esté establecido en la Unión lleva a cabo un tratamiento de datos personales interesados que sí residen en la Unión al tratarse de actividades de oferta de bienes y servicios.
- Actividades de observación del comportamiento
- "Derecho al olvido" en caso de infracción del Reglamento (Art. 17)
- Libertad de expresión e información (Art. 17.3.a)

Ya que el Derecho de Protección de datos NO supone un derecho absoluto y debe relacionarse con otros DDFF en base al principio de proporcionalidad, es correcto que cuando el gestor de un motor de búsqueda estime una solicitud de retirada de enlaces estará obligado a realizarla e las versiones de este que correspondan al conjunto de los EM combinando con medidas que impidan o dificulten el acceso a la lista de resultados objeto de la solicitud de retirada ("bloqueo geográfico").

- "Derecho de oposición" a que los datos sean objeto del tratamiento (Art. 21)
- Capítulo VII Reglamento 2016/679 (coherencia)

Art. 63. Mecanismo de coherencia: cooperación de las autoridades de control entre sí y con la comisión
Art. 65. Resolución de conflictos por el comité: una autoridad de control manifiesta una objeción pertinente y motivada o haya puntos de vista enfrentados.
Art. 66. Procedimiento de urgencia: medidas provisionales (3 meses)
Art. 60. Procedimiento de cooperación: intercambio de información, asistencia mutua, comunicación sin dilación de proyecto de decisión.
*Derecho francés - Ley 6 de enero de 1978
Art. 45: competencia del CNIL para requerir al responsable/encargado el fin del incumplimiento + posible sanción pecuniaria.

Cuestión prejudicial: en base "derecho al olvido" cuando el gestor de un motor de búsqueda estima una solicitud de retirada de enlaces debe hacerlo en todas las versiones de su motor de búsqueda o solo en ese Estado miembro + técnica "bloqueo geográfico".

Sentencia AN de 22 de noviembre de 2019: precisiones sobre la naturaleza del derecho al olvido —> debe ser apoyado e impulsado, pero tiene que haber una ponderación de hechos y medir los beneficios y bienes jurídicos a proteger.

Sentencia 1175/2020 de 17 de septiembre de 2020

"Como indica la doctrina, el derecho al olvido tiene como finalidad permitir a toda persona construir su vida sin la carga del pasado, por no concurrir un interés o utilidad social que justifique las consecuencias negativas asociadas a la publicidad de una noticia legítimamente divulgada en el pasado, cuando el transcurso del tiempo ha diluido el interés público subyacente en el mismo".
"Se fundamenta en que ciertas informaciones del pasado no continúen siendo difundidas cuando son capaces de provocar más daños que beneficios, de modo que hechos públicos, por razón del paso del tiempo, vuelven al área de privacidad o reserva, la esfera privada".
Lo cual comporta la existencia de un conflicto en el que se hace necesario un **juicio de valor o ponderación** de los derechos concurrentes, con la valoración de las circunstancias concurrentes a fin de considerar si el beneficio del ejercicio de la libertad de **información** o **expresión** es inferior a los daños provocados en otros bienes jurídicos".

En la **Sentencia 267/2019 de 26 de junio de 2019 (MUY IMPORTANTE)** de la Audiencia Provincial de Huelva se estableció que la incitación por parte de un adulto a una menor no es materia penal (en esa casuística especifica) "salvo en el caso de que se utilicen estas nuevas tecnologías para concertar encuentros siempre que la propuesta vaya acompañada de actos materiales de acercamiento". La sentencia concluyó que los "actos preparatorios quedarían impunes de no verificarse en ese ámbito especialmente peligroso del ciberdelito".

Problema: demostración del ciberdelito.

CONVENIO DE BUDAPEST

Convenio sobre Ciberdelincuencia de 24 de noviembre de 2001

Es la base. El inicio del proceso. Fue un convenio muy importante.

Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegitima de actos tales como producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos tipificados en los arts. de 2 a 5 del convenio.
Cualquier forma de puesta a disposición!!!!!!!
Arts 1-7 EXAMEN

Ilícitos digitales. Cada parte adoptará las medidas legislativas y de otro tipo que sean necesarias para tipificar como delito en su Derecho interno los siguientes casos:

Acceso ilícito (Art. 2): el acceso deliberado e ilegitimo a todo o parte de un sistema informático. Las partes podrán exigir que el delito se competa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.

Interceptación ilícita (Art. 3) IMPORTANTE
La interceptación deliberada e ilegitima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático desde un sistema informático o dentro del mismo.

Ataques a integridad de los datos (Art. 4)
Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.
“Todo acto deliberado e ilegitimo que dañe, borre o deteriore, altere o suprima datos informáticos”

Ataques a la integridad del sistema (Art. 5)
La obstaculizaron grave, deliberada e ilegitima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

DERECHOS DIGITALES

4 áreas relevantes: identidad, privacidad, desinformación, menores online.

- Ley 36/2015 de 28 de septiembre de Seguridad Nacional, que regula los principios y organismos fundamentales, así como las funciones que deben desempeñar para la defensa de la Seguridad Nacional. **Obsoleta**.
- Orden TIN 301672011 de 28 de octubre por la que se crea la Comisión de Seguridad en las Tecnologías de la Información y las Comunicaciones del MT e Inmigración. No ha servido.
- Ley 11/2002 de 6 de mayo reguladora del CNI - **sigue vigente**, ley muy buena
- Ley 9/1968 de 5 de abril sobre secretos oficiales - **sigue vigente**
- RD 1008/2017 por el que se aprueba la Estrategia de Seguridad Nacional (para cada año hay una nueva). Esta de 2017 muy importante. Marca un antes y un después
- LO de los estados de alarma, excepción y sitio
- Ley de secretos empresariales
- Estrategia nacional de ciberseguridad 2019 —> conjuga los recursos (aparato ciber). No tan importante como 2017.
- RD 3/2010 de 8 de enero por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Pionera, fue un hito.