uc3m | Universidad Carlos III de Madrid

ASIGNATURA: DERECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Coordinadora María Nieves de la Serna Bilbao
Prof[a] (PhD) Derecho Administrativo UC3M

LECCIÓN 9: EL DERECHO SANCIONADOR ADMINISTRATIVO Y PENAL; LAS TECNOLOGÍAS DE LA INFORMACIÓN

© 2021 *Por: PhD. FERNANDO FONSECA FERRANDIS*

Profesor Titular de Derecho Administrativo
Departamento Derecho Público del Estado
Universidad Carlos III de Madrid

Esta obra está bajo una licencia de Creative Commons Reconocimiento-NoComercial-CompartirIgual 3.0 España.

SUMARIO

1. Formas de control social del Estado de Derecho
2. Articulación competencial en la materia
3. Principio de legalidad
4. Principio de irretroactividad
5. Principio de tipicidad
6. Principio responsabilidad
7. Principio de proporcionalidad
8. Prescripción de infracciones y sanciones administrativas
9. Responsabilidad penal
10. Tipificación de los delitos relacionados con las TIC
11. Convenio sobre ciberdelincuencia del Consejo de Europa
12. Bibliografía

ABSTRACT

ABSTRACT

1.- Formas de control social del Estado de Derecho

- **Interés General** → normas limitadoras de la actuación de los diferentes sujetos
- Normas Penales/Normas Administrativas
- No identidad entre Función Punitiva y Organización Punitiva
  - Poder Judicial
  - Admón. Pública

Como es conocido, el régimen administrativo ha articulado un sistema de intervención o limitación de la actuación de los sujetos privados de derecho con el fin de preservar el interés general. Ahora bien, es preciso destacar que cuando tales mecanismos de intervención no resultan suficientes para la consecución de dicho fin, el mismo ordenamiento jurídico-administrativo prevé la posibilidad de que la propia Administración, sin necesidad de acudir al Poder Judicial pueda imponer sanciones; sanciones que, como todo acto administrativo, constituye un título administrativo directamente ejecutivo sin necesidad de acudir a la Jurisdicción contencioso-administrativa –autotutela ejecutiva-. De esta manera, nuestro ordenamiento establece un doble sistema represivo; el penal que se articula a través de normas penales y el administrativo que se ejecuta a través de normas administrativas.

No existe, pues, una unidad o identidad entre la función punitiva del Estado y la organización a la que se encomienda por principio el ejercicio de esta función. Si así fuera, el ejercicio de esta función debería haber quedado atribuido en exclusividad, de acuerdo con el dogma de la división de poderes, al Poder judicial. Sin embargo, como venimos destacando, el régimen administrativo ha reservado un importantísimo ámbito de facultades sancionadoras a la Administración pública. La conclusión es que existen dos centros o instancias de poder sancionador; el Poder judicial y la Administración pública.

Es preciso destacar que la existencia de un poder sancionador de naturaleza administrativa ha sido consagrad, por el art. 25.1 CE, que dispone expresamente que:
<<Nadie puede ser condenado o sancionado por acciones u omisiones que en el momento de su comsión no constituyan delito, falta o infracción administrativa… >>.

Igualmente ha sido reconocido por el Tribunal Constitucional (Ss. 42/1987, de 7-4; 133/1987, de 21-7; 26/1994, de 27-1, 117/1995, de 17-7 etc …) y por el Tribunal de Justicia de la Unión Europea (Ss. de 17-dic.-1970 –asunto 25/70, "Koester" y de 27-oct.-1992, aunto 240/90 Alemania /Comisión) que ha destacado expresamente que:

"La potestad sancionadora forma parte de la ejecución administrativa de las normas".

- **Poder Judicial** → Poder punitivo, entendido como (a) **delitos y faltas**, ejercido mediante (b) **condena** y que se traduce en una (c) **pena**.
- **Poder Administrativo** → Poder punitivo, respecto de (a) **infracciones advas**., ejercido mediante (**b) procedimiento advo./acto advo.** y que supone la imposición de (c) **sanciones administrativas**.

Como hemos destacado en la presentación anterior, nuestro ordenamiento jurídico-administrativo no establece un modelo judicialista puro en materia punitiva. D acuerdo con el principio de mínima intervención existen dos vías sancionadoras, cada una de las cuales corresponde a una instancia de poder público:

a) Poder Judicial: en relación con los delitos o faltas, ejercido mediante una condena y que se traduce en una pena.

b) Poder Administrativo: respecto de infracciones administrativas, ejercido a través del procedimiento administrativo (acto administrativo) y que supone la imposición de sanciones administrativas.

La materia relativa a protección datos no es una excepción a lo dicho.

2.- Articulación competencial en la materia

Art. 18.1 CE → LO (art. 81 CE) → Leg. Estatal.

Art. 149.1. 18 CE → Leg. Estatal:

- Bases del Régimen jurídico de las Admnes. Públicas [LRJSP (Tit. Preeliminar/Cap. III)].
- Procedimiento Administrativo Común [LPAC (Tít. IV/ Cap. II y V).

La competencia estatal para regular la actividad sancionadora de la Administración pública en materia de protección de datos resulta de la conjunción de dos circunstancias que es preciso destacar:

a) En primer lugar, es preciso destacar con carácter general que la protección de datos encuentra fundamento en el art. 18 de la Constitución relativo al derecho al honor, a la intimidad personal y a la propia imagen. Se trata, pues, de un derecho incluido en la Sección 1ª del Capítulo II del Título I y que, de acuerdo con una reiterada y unánime doctrina del Tribunal Constitucional, se trata de derechos que requieren ser regulados por ley orgánica. Se trata de una clase de ley que requiere un quorum especial y cuya aprobación está reservada al Congreso.

b) En segundo término, ya específicamente en lo que a la materia sancionadora se refiere, hay que destacar que encuentra fundamento constitucional en el art. 149.1. 18 de la Constitución que reserva al Estado la competencia para legislar las bases del régimen jurídico de las administraciones públicas y el procedimiento administrativo común, materias éstas en las que se inserta plenamente nuestro objeto de estudio. Recordemos que en desarrollo de dicho precepto constitucional la Ley 39/2015, de 1 de octubre de Procedimiento Administrativo Común de las Administraciones Públicas –en adelante, LPAC- y la Ley 40/2015, de 1 de octubre de régimen jurídico del Sector Público –LRJSP- han regulado el procedimiento común y el régimen jurídico al que se deben ajustar las administraciones en el desarrollo de su actividad formalizada con carácter pleno (común) el primero y básico el segundo. De tal circunstancia se derivaría una vinculación con tal carácter –según el objeto de la regulación- hacia el legislador

sectorial de protección de datos. No obstante, es preciso tener en cuenta en nuestro caso particular que Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales –en adelante, LOPDGDD- es el resultado del proceso de trasposición a nuestro derecho interno del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos, circunstancia de la que se desprende la pertenencia de la LOPDGDD a un sistema de fuentes distinto a nuestra legislación interna y relacionado con éste a través del principio de supremacía. A partir de dicha observación se entiende la previsión de la LOPDGDD cuando después de afirmar que las disposiciones de este Título –sobre el incumplimiento de la normativa en materia de protección de datos- son de aplicación a los procedimientos tramitados por la Agencia Española de Protección de Datos en los supuestos en los que un afectado reclame que no ha sido atendida su solicitud de ejercicio de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, así como en los que aquella investigue la existencia de una posible infracción, establece que los procedimientos tramitados por la Agencia Española de Protección de Datos se deben regir por lo dispuesto en el Reglamento (UE) 2016/679, en la LOPDGDD, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos. Evidentemente, estas normas de aplicación meramente supletorias son la LPAC y la LRJSP.

3. – Principio de legalidad

LRJSP

- 1. Reconocimiento expreso por **norma con rango de Ley** -> Cobertura necesaria y suficiente al ejercicio de la potestad sancionadora:

  – a) Elementos esenciales de la conducta antijurídica, de suerte que sólo infracciones las acciones u omisiones subsumibles en Ley formal.
  – b) Naturaleza y límites de las sanciones a imponer.

2. Ejercicio por los órganos administrativos. que la tengan expresamente atribuida por disposición legal o reglamentaria.

- 3. De acuerdo con el procedimiento previsto.

LOPDGDD

- Previsión expresa de la potestad sancionadora:

  – a) Art. 84 LOPDGDD =>definición de infracciones (acciones antijurídicas) y determinación de su naturaleza y límites.

  – b) Arts. 57 y 58 LOPDGDD => Previsión del ejercicio de la potestad sancionadora.

  – c) Arts. 44 y 47 LOPDGDD => Atribución expresa de la potestad sancionadora a la AEPD.

  – d) Art. 57 LOPDGDD => Posibilidad de atribución de potestad sancionadora a las Comunidades Autónomas.

Como es sabido, el principio de legalidad es el elemento nuclear del ejercicio por parte de las administraciones públicas. Se trata de que dicho reconocimiento esté previsto por una norma de rango legal que, además, debe definir al menos los caracteres esenciales y definidores de dicha potestad. Para todo el tráfico administrativo - con carácter básico-, la LRJSP consagra dicho principio cuyos principales aspectos son los siguientes:

1. La potestad sancionadora debe haber sido reconocida expresamente por norma con rango de Ley. No significa que no pueda entrar a regular la materia una norma reglamentaria, pero como hemos destacado con anterioridad, dicho texto legal debe proporcionar una cobertura necesaria y suficiente al ejercicio de la potestad sancionadora, circunstancia que se debe entender en un doble sentido:

a) Por un lado, debe contener los elementos esenciales de la conducta antijurídica, de suerte que sólo se pueden considerar infracciones las acciones u omisiones subsumibles en Ley formal.

b) Por otro, la ley debe definir la naturaleza y límites de las sanciones a imponer.

2. Una disposición legal o, en virtud de ésta, una norma reglamentaria, debe haber atribuido expresamente el ejercicio de la potestad a los órganos administrativos de que se trate.

3. El ejercicio de la potestad sancionadora se debe ejercer de acuerdo con el procedimiento previsto.

De acuerdo con dicha legislación básica, la LOPDGDD articula el principio de legalidad a partir de los siguientes extremos:

1. Arts. 57 y 58 LOPDGDD: Define las infracciones (acciones antijurídicas) y determina de su naturaleza y límites.
2. Arts. 44 y 47 LOPDGDD: Atribuye expresamente de la potestad sancionadora a la Agencia Española de Protección de Datos.
3. Art. 57 LOPDGDD: Contempla la posibilidad de que determinadas Comunidades Autónomas puedan asumir esta clase de competencia.

4.- Principio de Irretroactividad

LRJSP

1. Aplicación de las disposiciones sancionadoras vigentes en el momento de producirse los hechos constitutivos de infracción administrativa.

2. Aplicación retroactiva cuando favorezcan al presunto infractor.

Silencio de la Leg. Sectorial (LOPDGDD → aplicación directa de la LRJSP

El principio de irretroactividad exige la aplicación de la legislación vigente en el momento de la comisión de la infracción administrativa. Aparece consagrado a nivel constitucional cuando el art. 9.3 de la Constitución garantiza
<< ... el principio de legalidad, la jerarquía normativa, la publicidad de las normas, la irretroactividad de las disposiciones sancionadoras no favorables o restrictivas de derechos individuales, la seguridad jurídica la responsabilidad y la interdicción de la arbitrariedad de los poderes públicos.>>.
De este precepto es posible extraer ya, una primera conclusión. La retroactividad normativa que prohíbe nuestro ordenamiento jurídico es sólo aquella relativa a las disposiciones sancionadoras no favorables o restrictivas de derechos individuales, pero no aquélla que, por ejemplo, contenga una regulación más ventajosa. Esta última sí que es objeto de regulación retroactiva.

La LRJSP se refiere al principio de irretroactividad desde dos puntos de vista:

1. En primer lugar, consagra la regla general de la aplicación de las disposiciones sancionadoras vigentes en el momento de producirse los hechos constitutivos de infracción administrativa.

2. En segundo, establece la retroactiva cuando –como ya sabemos- favorezcan al presunto infractor.

Dado el silencio en este punto de la legislación sectorial, es decir, de la LOPDGDD, procede en este punto la aplicación directa de la LRJSP.

5. – Principio de tipicidad

LRJSP

Solo son infracciones administrativas las vulneraciones del ordenamiento jurídico *previstas como tales infracciones por una Ley*:

a) Ley formal debe calificar los supuestos como "infracciones".
b) Clasificar éstas en leves, graves o muy graves.

2. Sanciones deben estar *delimitadas por Ley* => mayor margen de libertad al legislador => colaboración del Rgto:

a) Ley formal debe establecer directamente cuadro de infracciones o sanciones.
b) Rgto. no puede:
- prever nuevas infracciones o sanciones (especificar o graduar éstas).
-alterar la naturaleza o los límites impuestos por la Ley forma.

3. Normas definidoras de Infracciones y sanciones nunca susceptibles de aplicación analógica.

LOPDGDD

1. Constituyen infracciones los actos y conductas a las que se refieren los aps. 4, 5 y 6 del art. 83 RGPD, así como las que resulten contrarias a la LOPDGDD.

Remisión a las previsiones generales del RGPD (art. 71 LOPDGDD).
Desarrollo general de las previsiones del RGPD (art. 84.4, 5 y 6 LOPDGDD).

2. Definidas en la LOPDGDD:

a) Multa de hasta 10.000.000 euros o el 2% del volumen total anual global del ejercicio.
b) Multa de hasta 20.000.000 euros o el 4% del volumen total anual global del ejercicio.
c) Multa de hasta 20.000.000 euros o el 4% del volumen total anual global del ejercicio.

NO PREVISIÓN REGLAMENTARIA

De acuerdo con lo previsto en la LRJSP, sólo son infracciones administrativas las vulneraciones del ordenamiento jurídico << … *previstas como tales infracciones por una Ley.* >>. Desde este punto de vista y, en aras a dar cabal cumplimiento a tal mandato, tanto la jurisprudencia contencioso-administrativa, como la doctrina, han considerado necesario, que la ley (formal) cumpla dos extremos:

a) En primer lugar, la ley debe calificar expresamente tales supuestos como "infracciones".

b) En segundo, debe clasificar dichas infracciones como leves, graves o muy graves.

Es preciso destacar que la exigencia de ley, lo es –como hemos destacado- en sentido formal, circunstancia que impide la concurrencia en este punto de una norma meramente reglamentaria. No obstante, la propia LRJSP introduce cierta minoración en esta exigencia al prever que las disposiciones administrativas de desarrollo puedan introducir especificaciones al cuadro de sanciones previsto legalmente. Por tanto, el reglamento no puede establecer sanciones nuevas, no previstas legalmente pero sí, a partir de las previstas por la ley, establecer ciertas modulaciones o especificaciones, acordes, claro está, con aquéllas.

Tratándose de la determinación de las subsiguientes sanciones, nuestro ordenamiento jurídico ha sido tradicionalmente menos exigente en relación con el protagonismo de la ley reduciendo éste a delimitar la sanción, tenor que reconoce implícitamente la colaboración del reglamento. La LRJSP confirma esta línea cuando acepta que la norma reglamentaria pueda establecer graduaciones al cuadro de de sanciones establecidas legalmente. En ambos casos se trata de contribuir a una más correcta identificación de las conductas o a la más precisa determinación de las sanciones. En cualquier caso, existen dos límites que no poder ser rebasados:

a) Es la Ley formal la norma que debe establecer inicialmente el cuadro de infracciones o sanciones.

b) El reglamento no puede, ni prever nuevas infracciones o sanciones (se debe limitar a especificar o graduar éstas), ni alterar la naturaleza o los límites impuestos por la Ley.

En cualquier caso, es preciso destacar que como ocurre en el derecho penal, las normas definidoras de Infracciones y sanciones administrativas nunca susceptibles de aplicación analógica.

En relación con la LOPDGDD hay que señalar que su articulado cumple satisfactoriamente con estos requisitos y establece las siguientes infracciones y sanciones:

a) Infracciones sancionadas con multas de 10.000.000 euros como máximo o tratándose de una empresa, con una cuantía equiv al 2% como máximo del volumen de negocio total anual global del ejercicio anterior, optándose por la de mayor cuantía:

i) Las obligaciones del responsable y del encargado (arts. 8, 11, 25 a 39, 42 y 43).
ii) Las obligaciones de los organismos de certificación (arts. 42 y 43).
iii) Las obligaciones de la autoridad de control (art. 41.4).

b) Infracciones sancionadas con multas de 20.000.000 euros como máximo o tratándose de una empresa, con una cuantía equiv al 4% como máximo del volumen de negocio total anual global del ejercicio anterior, optándose por la de mayor cuantía:
i) Los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento (arts. 5, 6, 7 y 9).
ii) Los derechos de los interesados (arts. 12 a 22).
iii) Las transferencias de datos personales a un destinatario en un tercer país o una organización internacional (arts. 44 a 49).
iv) Toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al Capítulo IX (sobre "*Situaciones específicas de tratamiento*").
v) El incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control (art. 58.2) o no facilitar acceso en incumplimiento del art. 58.1.

c) Finalmente, el incumplimiento de las resoluciones de la autoridad de control, a tenor del art. 58.2 (*poderes correctivos*) se sanciona con multa de 20.000.000 euros como máximo o, tratándose de una empresa de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.
No existen previsiones reglamentarias al respecto.

6. – Principio de responsabilidad

LRJSP

- 1. **Responsabilidad personal o subjetiva**.

- 2. **Responsabilidad solidaria** => Siempre que la obligación legal cuyo incumplimiento determina la infracción recaiga sobre varias personas conjuntamente.

- 3. **Responsabilidad subsidiaria** => Siempre que la obligación cuyo incumplimiento determina la infracción, comporte el deber de prevenir la infracción administrativa por terceros.

LOPDGDD

- Sujetos responsables => **responsables de los ficheros y los encargados de los tratamientos** (art. 70 LOPDGDD).

El principio de responsabilidad, propio del Derecho Penal, rige también en el ámbito administrativo sancionador. Así lo tiene establecido una unánime y reiterada doctrina del Tribunal Constitucional. Constitucionalmente queda excluida una responsabilidad meramente objetiva y, por tanto, resultan inconstitucionales todas las normas que impongan una responsabilidad de este tipo. La responsabilidad es siempre personal o subjetiva, es decir, se requiere dolo, culpa o, en su caso, la omisión de toda diligencia exigible en el cumplimiento de la normativa administrativa. La responsabilidad, además de subjetiva, es solidaria. Siempre que la obligación legal cuyo incumplimiento determina la infracción recaiga sobre varias personas conjuntamente, se exige a todas éstas.

Finalmente, es preciso destacar que se trata de una responsabilidad de carácter subsidiario, es decir, siempre que la obligación cuyo incumplimiento determina la infracción, comporta el deber de prevenir la infracción administrativa por terceros.

La LOPDGDD es muy escueta sobre esta cuestión y se limita a determinar como sujetos responsables de las infracciones administrativas de que se trate, a los responsables de los ficheros y los encargados de los tratamientos. En todo lo no previsto por este texto legal, resulta aplicable la LRJSP.

7. – Principio de proporcionalidad

LRJSP

Debida adecuación entre la gravedad del hecho constitutivo de la infracción y la sanción aplicada:

Existencia de intencionalidad.
Naturaleza de los perjuicios causados.
Reincidencia.

LOPDGDD

1. Graduación de cuantía de las sanciones atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos afectados, a los beneficios obtenidos, al grado de intencionalidad, reincidencia, daños y perjuicios causados o cualquier otra circunstancia relevante para determinar el grado de antijuricidad y de culpabilidad presentes en la concreta actuación infractora

2. Aplicación de la escala de la sanción menos graves => atendiendo a circunstancias concurrentes, se aprecia una cualificada disminución de la culpabilidad del imputado o de la antijuricidad del hecho.

El principio de proporcionalidad es un principio sustancial del Estado de Derecho, directamente relacionado con el de interdicción de la arbitrariedad de los poderes públicos al que se refiere el art. 9.3 de la Constitución. Como tal exige que exista una adecuación entre la gravedad del hecho constitutivo de la infracción y la sanción

aplicada. De ahí que resulte un principio muy relevante en determinados ámbitos del tráfico administrativo en los que, como es el caso, puede estar afectado el orden público. La LRJSP se refiere al principio de proporcionalidad desde tres puntos de vista:

a) La existencia de intencionalidad o reiteración.

b) La naturaleza de los perjuicios producidos.

c) La reincidencia, por la comisión en el término de un año de más de una infracción de la misma naturaleza, cuando así haya sido declarado por resolución firme.

En cualquier caso, es preciso tener en cuenta dos reglas que vienen igualmente a incidir en el principio de proporcionalidad:

a) En primer lugar, que las sanciones administrativas sean o no de naturaleza pecuniaria, en ningún pueden implicar, directa o subsidiariamente, privación de libertad

b) En segundo, que el establecimiento de sanciones pecuniarias debe prever que la comisión de las infracciones tipificadas no resulte más beneficioso para el infractor que el infractor que el cumplimiento de las normas infringidas.

La LOPDGDD da cumplimiento al principio de proporcionalidad, de acuerdo con la LRJSP, mediante el establecimiento de las siguientes reglas:

a) La graduación de cuantía de las sanciones se debe realizar atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos afectados, a los beneficios obtenidos, al grado de intencionalidad, reincidencia, daños y perjuicios causados, o cualquier otra circunstancia relevante para determinar el grado de antijuricidad y de culpabilidad presentes en la concreta actuación infractora.

b) Se debe aplicar la escala de la sanción menos graves, atendiendo a circunstancias concurrentes, se aprecia una cualificada disminución de la culpabilidad del imputado o de la antijuricidad del hecho.

c) En ningún caso se puede aplicar una sanción más grave que la que corresponde aplicar.

8. – Prescripción de infracciones y sanciones administrativas

Como novedad, la LRJSP establece un régimen general de prescripción de infracciones y sanciones administrativas de la siguiente forma:

Infracciones:	Sanciones:
a) Muy graves => 3 años.	a) Muy graves => 3 años.
b) Graves => 2 años.	b) Graves => 2 años.
c) Leves => 6 meses.	c) Leves => 1 años.

Tal régimen no es de directa aplicación a todas las infracción dado que el establecimiento de éstos queda remitido a lo dispuesto en la legislación sectorial. En este sentido, dicho texto legal dispone que las infracciones y las sanciones prescriben según lo dispuesto en las leyes que las establezcan.

La LOPDGDD adopta casi a pie juntillas estos plazos, de acuerdo con el siguiente esquema:

Infracciones:	Sanciones
a) Muy graves =>3 años.	a) Muy graves =>3 años.
b) Graves =>2 años.	b) Graves =>2 años.
c) Leves =>1 año.	c) Leves =>1 año.

En el caso de las infracciones el plazo de prescripción comienza a computar desde el día en que se cometió la infracción. En el caso de las sanciones, el pazo de prescripción comienza a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impuso la sanción.

9.- Responsabilidad Penal

Código Penal → Se reconoce la necesidad de introducir nuevas figuras delictivas y la desaparición o modificación de aquellas figuras, ya desfasadas, que habían perdido su razón de ser.

↓

Todo acto que se vale de las TIC para su comisión

En la Exposición de Motivos del Código Penal –Ley Orgánica 10/1995, de 23 de noviembre, modificada sucesivamente- se reconoce la necesidad de tutelar valores y principios básicos de la convivencia social. De esta forma considera que cuando los valores y principios cambian las leyes también deben cambiar, y por ello corresponde al legislador introducir nuevas figuras delictivas y proceder a modificar o hacer desaparecer aquellas figuras, ya desfasadas, que han perdido su razón de ser. De acuerdo con lo anteriormente expuesto, el legislador español procedió a regular nuevos hechos que preocupan a la sociedad, y en lo que a nosotros interesa, aquellos que utilizan las Tecnologías de la Información y las comunicaciones para la realización o comisión de delitos. Sin embargo, es preciso indicar que en el Código Penal no encontramos un Capítulo o Titulo donde se recojan expresamente los delitos relacionados con las TIC. Ello no es óbice para que podamos destacar que la existencia de una reacción penal al problema, a través de todas aquellas actuaciones en las que se utilizan las TIC para la comisión de delitos.

10.- Tipificación de los delitos relacionados con las TIC

El Código penal no contiene un Título o un Capítulo específico que regule los delitos TIC. Por el contrario, a lo largo de todo Código Penal existen diversos artículos que regulan los delitos TIC.

Lo importante en este caso es que se cometan o utilicen las TIC para cometer el delito.

Los delitos relacionados con las TIC, se pueden definir con carácter general como toda actuación que se vale de las TIC para su comisión o que tiene como fin estos bienes. En toda comisión de los delitos relacionados con las TIC es necesario proceder a distinguir el **medio y el fin** por el que se cometen. Así para poder considerar que una acción es dolosa o imprudente dentro de este tipo de delitos, el **medio** por el que se cometen debe estar directamente vinculado con las TIC. Asimismo, en relación con el **fin** que se persiga con la comisión en estos delitos, es preciso indicar que el sujeto autor del ilícito, debe buscar un beneficio o tener como finalidad causar un perjuicio a otro o a un tercero. Es imposible en este trabajo tratar de analizar todos; nos limitaremos a analizar tan solo a algunos de ellos:

a) Los delitos recogidos en el Título X denominado "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en cuyo Capítulo I " Del descubrimiento y revelación de secretos".

Artículo 197 CP:

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años

……

5. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

6. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

……

b) TITULO XIII, Delitos contra el patrimonio y contra el orden socioeconómico, Capítulo II de los Robos

El artículo 238

Son reos del delito de robo con fuerza en las cosas los que ejecuten el hecho cuando concurra alguna de las circunstancias siguientes:

4.º Uso de llaves falsas.

Artículo 239.

A los efectos del artículo anterior, junto a otros supuestos, se consideran llaves falsas las tarjetas, magnéticas o perforadas, los mandos o instrumentos de apertura a distancia y cualquier otro instrumento tecnológico de eficacia similar

c) CAPÍTULO VI De las defraudaciones, *Sección 1.ª De las estafas*

Artículo 248.2.

Se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

d) CAPÍTULO IX. De los daños

Artículo 264.

1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o

documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a dos años.

2. El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años.

e) CAPÍTULO XI De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores. *Sección 1.ª De los delitos relativos a la propiedad intelectual*

Artículo 270.

1. Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

……

3. Será castigado también con la misma pena quien fabrique, importe, ponga en circulación o tenga cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador o cualquiera de las otras obras, interpretaciones o ejecuciones en los términos previstos en el apartado 1 de este artículo.

f) *Sección 3.ª De los delitos relativos al mercado y a los consumidores*

Artículo 278.

1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se

refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

Artículo 286.

1. Será castigado con las penas de prisión de seis meses a dos años y multa de seis a 24 meses el que, sin consentimiento del prestador de servicios y con fines comerciales, facilite el acceso inteligible a un servicio de radiodifusión sonora o televisiva, a servicios interactivos prestados a distancia por vía electrónica, o suministre el acceso condicional a los mismos, considerado como servicio independiente, mediante:

1.º La fabricación, importación, distribución, puesta a disposición por vía electrónica, venta, alquiler, o posesión de cualquier equipo o programa informático, no autorizado en otro Estado miembro de la Unión Europea, diseñado o adaptado para hacer posible dicho acceso.

2.º La instalación, mantenimiento o sustitución de los equipos o programas informáticos mencionados en el párrafo 1.º

2. Con idéntica pena será castigado quien, con ánimo de lucro, altere o duplique el número identificativo de equipos de telecomunicaciones, o comercialice equipos que hayan sufrido alteración fraudulenta.

g) TÍTULO XVIII, De las falsedades, CAPÍTULO II Disposiciones generales

Artículo 400.

La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

Es preciso destacar al margen de los ejemplos citados que, en algunos casos, el propio tipo no contempla específicamente el uso de las TIC pero la realización de la acción por tales medios, si conlleva la aplicación del tipo. Así, por ejemplo, todos aquellos casos en los que se menciona la difusión o exhibición, hechos que pueden realizarse a través de TIC. Ejemplos:

Artículo 186.
El que, por cualquier medio directo, vendiere, difundiere o exhibiere material pornográfico

Artículo 189 que indica expresamente *"cualquiera que sea su soporte":*
1. Será castigado con la pena de prisión de uno a cinco años:

a) El que captare o utilizare a menores de edad o a incapaces con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas.

Otro ejemplo es el artículo 578 del Código Penal que regula la apología del terrorismo como delito, en los siguientes términos:

"El enaltecimiento o la justificación por cualquier medio de expresión pública o difusión de los delitos comprendidos en los artículos 571 a 577 de este Código o de quienes hayan participado en su ejecución, o la realización de actos que entrañen descrédito, menosprecio o humillación de las víctimas de los delitos terroristas o de sus familiares se castigará con la pena de prisión de uno a dos años."

La Jurisprudencia ha considerado, por ejemplo, que quien realiza apología del terrorismo por medio del uso de las redes sociales, como Twitter, Facebock, etc., comete este delito.

Al margen de la cuestión anterior, es preciso indicar que existen distintas actuaciones que están directamente relacionadas con el ámbito penal pero no se encuentran recogida en el Código Penal. Un ejemplo de ello es la regulación contenida en la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género, que determina la obligación publicitaria de respetar la dignidad de las mujeres y el derecho a una imagen no estereotipada, ni discriminatoria, tanto en los medios de comunicación públicos como en los privados. De otro lado, se refuerza la acción de cesación o rectificación de la publicidad y con tal finalidad se legitima a las instituciones y asociaciones que trabajan a favor de la igualdad entre hombres y mujeres para su ejercicio.

Otro ejemplo es la Ley orgánica 10/2007, de 8 de octubre, reguladora de las Bases de Datos Policiales sobre identificadores obtenidos a partir del ADN que regula la creación y utilización por parte de las Fuerzas y Cuerpos de Seguridad del Estado de la información que el ADN puede ofrecer a nivel de identificación personal. La mencionada norma posibilita la inscripción en dicha base de datos de los siguientes:

a) Los datos identificativos extraídos a partir del ADN de muestras o fluidos que, en el marco de una investigación criminal, hubieran sido hallados u obtenidos a partir del análisis de las muestras biológicas del sospechoso, detenido o imputado, cuando se trate de delitos graves y, en todo caso, los que afecten a la vida, la libertad, la indemnidad o la libertad sexual, la integridad de las personas, el patrimonio siempre que fuesen realizados con fuerza en las cosas, o violencia o intimidación en las personas, así como en los casos de la delincuencia organizada, debiendo entenderse incluida, en todo caso, en el término delincuencia organizada la recogida en el artículo 282 bis, apartado 4 de la Ley de Enjuiciamiento Criminal en relación con los delitos enumerados.

b) los patrones identificativos obtenidos en los procedimientos de identificación de restos cadavéricos o de averiguación de personas desaparecidas.

La inscripción en la base de datos policial, no precisa el consentimiento del afectado que es informado por escrito de todos los derechos que le asisten respecto a la inclusión en dicha base, quedando constancia de ello en el procedimiento. No obstante, también es posible inscribir los datos identificativos obtenidos a partir del ADN cuando el afectado hubiera prestado expresamente su consentimiento.

Los datos contenidos en la base de datos de ADN, puede ser utilizada exclusivamente por las Unidades de Policía Judicial de las Fuerzas y Cuerpos de Seguridad del Estado -Policía Nacional y Guardia Civil- y por ciertas autoridades Judiciales y Fiscales, en la investigación de los delitos. Igualmente, es posible ceder los datos contenidos en la base de datos analizada en los siguientes supuestos:

a) Cuando se trate de las Autoridades Judiciales, Fiscales o Policiales de terceros países de acuerdo con lo previsto en los convenios internacionales vigentes.

b) En el caso de las policías autonómicas para la protección de personas y bienes y para el mantenimiento de la seguridad pública o, en su caso, para la identificación de cadáveres o averiguación de personas desaparecidas.

c) También se pueden ceder al Centro Nacional de Inteligencia (CNI), que puede utilizar los datos para el cumplimiento de sus funciones relativas a la prevención de tales delitos.

11.- El Convenio sobre Ciberdelincuencia del Consejo de Europa

- Convenio de Ciberdelincuencia del Consejo de Europa firmado el 23 de noviembre del 2001 en Budapest.

Es el mayor consenso, hasta la fecha, sobre la comisión de delitos por medio de las TIC.

El Convenio de Ciberdelincuencia del Consejo de Europa -adoptado por el Comité de Ministros el 8 de noviembre de 2001, firmado en Budapest, el 23 de noviembre de 2001 y entra en vigor el 1 de julio de 2004[1]- tiene por finalidad proteger a la sociedad frente a la ciberdelincuencia. Se trata de un documento en el que existe el mayor consenso, hasta la fecha, sobre la comisión de delitos por medio de las TIC. Asimismo, persigue recoger una política penal común y adoptar una legislación que fomente la cooperación internacional en la materia. Con esta finalidad, establece el deber de adoptar las medidas legislativas -o, de cualquier otro tipo- que resulten necesarias para que el derecho interno de cada Estado miembro tipifique como delito las acciones descritas en el Convenio. En cualquier caso, resulta de gran interés dado que reflexiona sobre los profundos cambios que ha supuesto la digitalización, la convergencia y la globalización de las redes informáticas para la sociedad y la utilización de aquellas para cometer delitos o para almacenar o trasmitir por medio de dichas redes las pruebas de los delitos cometidos.

[1] El Convenio de Ciberdelincuencia fue firmado por los países participantes pero tan solo ratificado por ocho países: Albania (20-6-02), Croacia (17-10-02), Estonia (12-5-03), Hungría (4-12-03), Lituania (2-03-04), Rumania (12-5-04), Eslovenia (8-9-04) y Macedonia (15-9-04).

En el citado Convenio se concretan las medidas que a nivel nacional se deben adoptar y que se trata de los siguientes:

a) **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos**, dentro de los cuales se incluye:

i).- El acceso ilícito, es decir, el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Las Partes pueden exigir que el delito se cometa 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.

ii).- La interceptación ilícita, es decir, la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Las Partes pueden exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

iii).- La interferencia en los datos, la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

iv).- La interferencia en el sistema, la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

v).- El abuso de los dispositivos, es decir, la comisión deliberada e ilegítima de los siguientes actos: a) La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos antes mencionados; una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático; b) la posesión de alguno de los elementos mencionados con anterioridad

con el fin de que sean utilizados para cometer cualquiera de los delitos previstos antes mencionados.

b) **Delitos informáticos**, dentro de estos se incluyen:

i) La falsificación informática, es decir, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles.

ii) El fraude informático, los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: a) Cualquier introducción, alteración, borrado o supresión de datos informáticos; b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

c) **Delitos relacionados con el contenido**, que comprende:

i) Delitos relacionados con la pornografía infantil, que comprende todo material pornográfico que contenga la representación visual de un menor comportándose de una forma sexualmente explícita; una persona que parezca un menor comportándose de una forma sexualmente explícita; e imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita. Dentro de este delito se comprende la comisión deliberada e ilegítima de los siguientes actos: a) La producción de pornografía infantil con vistas a su difusión por medio de un sistema informático; b) la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático; c) la difusión o transmisión de pornografía infantil por medio de un sistema informático; d) la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona; e) la posesión de pornografía infantil en un sistema informático o en un medio. En todos estos casos se entiende por menor toda persona menor de dieciocho años, o de un límite de edad inferior, que será como mínimo de dieciséis años.

d) **Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines,** teniendo en cuenta los siguientes extremos:

i) Las obligaciones asumidas en aplicación del Acta de París de 24 de julio de 1971 por la que se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre la propiedad intelectual, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

ii) Las obligaciones que ésta haya asumido en aplicación de la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre las obras de los intérpretes y ejecutantes y los fonogramas, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

El Convenio también recoge otras formas de responsabilidad como corresponde a los cómplices y a las personas jurídicas. Igualmente indica que las medidas legislativas deben conducir a que los delitos, sanciones o medidas penales o no penales sean efectivas, proporcionadas y disuasorias, según los hechos cometidos.

Finalmente, hay que destacar el Convenio analizado autoriza a las Partes para adoptar medidas legislativas sobre el "Registro y confiscación de datos informáticos almacenados", la "Obtención en tiempo real de datos informáticos" y la "Interceptación de datos sobre el contenido".