RESUMEN TEORÍA DEONTOLOGÍA Y NORMATIVA EN ROBÓTICA:

TEMAS 1 Y 2:

- **1.1 EL ESTADO DE DERECHO**
  - **1.1.1 LA CONSTITUCIÓN ESPAÑOLA**
  - **1.1.2 LEYES Y PRINCIPIOS SUPERIORES**
- **1.2 VALORES SUPERIORES Y PRINCIPIOS CONSTITUCIONALES**
  - **1.2.1 SEGURIDAD**
  - **1.2.2 LIBERTAD**
  - **1.2.3 IGUALDAD**
  - **1.2.4 SOLIDARIDAD**
- **1.3 DERECHOS DE PERSONALIDAD (LA INTIMIDAD)**
  - **1.3.1 INTIMIDAD CONSTITUCIONAL**
  - **1.3.2 INTIMIDAD SEGÚN PROSSER**
- **1.4 REGLAMENTO UE PROTECCIÓN DE DATOS**
  - **1.4.1 ARTÍCULO 12**
  - **1.4.2 ARTÍCULO 13**
  - **1.4.3 ARTÍCULO 14**
  - **1.4.4 ARTÍCULO 15**
  - **1.4.5 ARTÍCULO 16**
  - **1.4.6 ARTÍCULO 17**
  - **1.4.7 ARTÍCULO 18**
- **1.5 LEY DE PROTECCIÓN DE DATOS DE 2018**
  - **1.5.1 ARTÍCULO 28**
  - **1.5.2 ARTÍCULO 33**

TEMAS 3 Y 4:

- **2.1 PRIMER PUNTO DE DISCUSIÓN SOBRE CÓDIGOS DEONTOLÓGICOS**
- **2.2 CÓDIGO ÉTICO INGENIEROS ROBÓTICA UE**
- **2.3 CÓDIGO DEONTOLÓGICO INGENIERÍA INFORMÁTICA**
  - **2.3.1 PRINCIPIOS DEONTOLÓGICOS UNIVERSALES**
  - **2.3.2 RESPONSABILIDAD PROFESIONAL**
  - **2.3.3 ARTÍCULO 7**
  - **2.3.4 ARTÍCULO 8**
  - **2.3.5 ARTÍCULO 13**
  - **2.3.6 ARTÍCULO 16**
  - **2.3.7 ARTÍCULO 17**

TEMAS 5 Y 6:

- **3.1 CONSIDERACIONES ÉTICAS DE LA INTELIGENCIA ARTIFICIAL**
  - **3.1.1 ÉTICA Y TÉCNICA**
  - **3.1.2 EL ARMA DE LA ÉTICA**
  - **3.1.3 ¿QUÉ ES LA IA?**
  - **3.1.4 ¿REEMPLAZARÁN AL SER HUMANO LOS ROBOTS DOTADOS DE IA?**
  - **3.1.5 ¿DÓNDE SE ESTÁ DESARROLLANDO LA IA?**
- **3.2 PUNTOS DE DISCUSIÓN SOBRE ROBÓTICA PRINCIPIOS 2017**
  - **3.2.1 ¿VA A INCIDIR LA ROBÓTICA EN EL ÁMBITO LABORAL Y LA EMPLEABILIDAD?**
  - **3.2.2 ¿VAN A INCIDIR LA ROBÓTICA Y LA IA EN EL ÁMBITO SOCIAL Y POLÍTICO?**
- **3.3 REGLAMENTO EUROPEO INTELIGENCIA ARTIFICIAL**
  - **3.3.1 ARTÍCULO 5**
  - **3.3.2 ARTÍCULO 6**

TEMAS 7 Y 8:

- **4.1 INTELIGENCIA ARTIFICIAL Y ROBÓTICA (NORMATIVA Y RETOS)**
  - **4.1.1 LA UNIÓN EUROPEA Y LA INTELIGENCIA ARTIFICIAL**
  - **4.1.2 CUATRO GRANDES HITOS DE LA UNIÓN EUROPEA**
  - **4.1.3 CREACIÓN DE AGENCIAS Y LEGISLACIÓN SOBRE IA**
  - **4.1.4 ÁMBITO LABORAL**
  - **4.1.5 LEY DE IGUALDAD DE TRATO**
  - **4.1.6 PAPEL DE LA IA EN LOS MODELOS DE GOBERNANZA**
  - **4.1.7 REQUISITOS ESENCIALES PARA LOGRAR UNA IA FIABLE**
- **4.2 REGISTRO DE ROBOTS, IA Y UE**
  - **4.2.1 EL DERECHO DE LOS ROBOTS INTELIGENTES**
  - **4.2.2 BASES PARA CONSEGUIR LA PERSONALIDAD ELECTRÓNICA**
  - **4.2.3 EL REGISTRO DE ROBOTS INTELIGENTES Y LA CREACIÓN DE FONDOS**
  - **4.2.4 ROBOTS INTELIGENTES Y LICENCIAS DE USO DE LA INTELIGENCIA ARTIFICIAL**

TEMAS 9 Y 10:

- **5.1 RESPONSABILIDAD CIVIL Y PENAL**
- **5.2 CÓDIGO PENAL 2023**
  - **5.2.1 ARTÍCULO 116**
  - **5.2.2 ARTÍCULO 117**
  - **5.2.3 ARTÍCULO 197**
  - **5.2.4 ARTÍCULO 278**
  - **5.2.5 ARTÍCULO 280**
- **5.3 REGLAMENTO RC IA**
  - **5.3.1 ARTÍCULO 4**
  - **5.3.2 ARTÍCULO 5**
  - **5.3.3 ARTÍCULO 6**
  - **5.3.4 ARTÍCULO 8**

OTROS RECURSOS:

- **6.1 CONSTITUCIÓN ESPAÑOLA**
  - **6.1.1 ARTÍCULO 1**
  - **6.1.2 ARTÍCULO 9**
  - **6.1.3 ARTÍCULO 10**
  - **6.1.4 ARTÍCULO 14**
  - **6.1.5 ARTÍCULOS DEL 15 AL 29**

[] TEMAS 1 Y 2:

[] 1.1 EL ESTADO DE DERECHO

} 1.1.1 LA CONSTITUCIÓN ESPAÑOLA

La Constitución Española es la norma Suprema del ordenamiento jurídico español y ésta sólo puede modificarse conforme al procedimiento que ella misma prevé.
Las normas del estado español pueden resumirse en una pirámide, la cual está compuesta por los siguientes elementos: Constitución, tratados internacionales, leyes orgánicas y ordinarias, decretos legislativos y de ley, reglamentos del gobierno, leyes y reglamentos de las comunidades autónomas.
Éstas otras a su vez se subdividen respecto a especialidades o competencias siempre dentro de la pirámide (cada una recibe un nombre según lo que trate). Se tienen 2 grupos muy importantes:
Derecho privado: Derecho civil, mercantil, laboral e internacional privado.
Derecho público: Derecho constitucional, penal, administrativo e internacional público.

} 1.1.2 LEYES Y PRINCIPIOS SUPERIORES

Debajo de la Constitución están las Leyes Orgánicas (Estatutos de Autonomía), que crean diversos sistemas con una enorme competencia en muchos temas distintos (Código Penal o Ley de Régimen Electoral General). No solo están éstas, ya que también tenemos las Leyes Ordinarias (Código Civil, Estatuto de Trabajadores o Leyes de Minería, Pesca, Medicina, Ingeniería o Economía), todas creadas de forma jerárquica.
Estas leyes deben ser creadas por distintas organizaciones (siempre con jerarquía), así como el Congreso de los Diputados o los distintos organismos de las comunidades autónomas, éstos últimos con menos poder.
Principios superiores: Se denominan así porque además de ser respetados y cumplidos por todos, sirven para interpretar y aplicar todas las normas del Ordenamiento (Dignidad del hombre, Justicia, Igualdad, Libertad, Seguridad Jurídica y Solidaridad).
Derechos Fundamentales: Están al mismo nivel, se encuentran en la primera sección (del 15 al 29).
Derechos Constitucionales: Son los que se encuentran en la segunda sección (del 30 al 38).
Derechos Latentes: Son los de la tercera sección y sólo se puede acudir a ellos cuando la legislación los desarrolla, también sirven para interpretar el derecho pero dependen de las leyes que los regulan (del 39 hasta el final).
La jerarquía y características de todos ellos se definen en el artículo 53 de la Constitución.

[] 1.2 VALORES SUPERIORES Y PRINCIPIOS CONSTITUCIONALES

} 1.2.1 SEGURIDAD

Seguridad jurídica (9.1 y 9.3): Surge a lo largo del siglo XIX y se sitúa como respuesta a las relaciones de los hombres con otros y su entorno, con el objetivo de cohesión e integración, simplemente para liberar al hombre del temor y producir certeza a través de cuerpos públicos, siempre vinculada a otro valor (Libertad).

} 1.2.2 LIBERTAD

Libertad (1.1): Tiene mucho que ver con la dignidad del hombre y da la posibilidad de elegir en el ámbito privado tus creencias. Podemos distinguir entre libertad de elección (base y condición de la moralidad) y libertad moral (meta ideal a alcanzar, siendo el buen resultado de la anterior).
Libertad social, política y jurídica: Es libertad para hacer lo que se quiera y para intervenir en la formación de los criterios de decisión de lo que se debe hacer, ningún organismo público debe intervenir en ello y posee una relación muy estrecha con la intimidad.

} 1.2.3 IGUALDAD

Igualdad (1.1): Es complementaria a la libertad.
Igualdad formal: Todas las personas son sujetos de derecho, no existe el privilegio entre ciudadanos y todos tenemos las mismas normas (igualdad procesal). Según el caso dado podemos tener la igualdad como equiparación (la de toda la vida) o la igualdad como diferenciación (se deben tener en cuenta ciertos aspectos como por ejemplo la edad).
Igualdad material: Medio para llegar a la libertad moral (ningún hombre es tan rico como para comprar a otro ni tan pobre como para venderse).

} 1.2.4 SOLIDARIDAD

Solidaridad (9.2): Surge a finales del siglo XVIII (relacionado con la misericordia), se basa en actuar a favor del ser humano para contribuir a la libertad moral y al desarrollo de la dignidad. Se refiere al individuo como un ser que vive en una sociedad jurídica organizada para ayudar a terceros, por eso hay ayudas para las personas (no se debe confundir con la igualdad o la libertad promocional).

[] 1.3 DERECHOS DE PERSONALIDAD (LA INTIMIDAD)

} 1.3.1 INTIMIDAD CONSTITUCIONAL

Derecho a la Intimidad en la Constitución: Derecho que tenemos a lo nuestro (autonomía, libertad y privacidad), todo ello de manera informal ya que no es lo suficientemente estricto como para ser aplicable al derecho, además de que no se distingue muy bien del derecho al honor y a la propia imagen.
Según la Asamblea Parlamentaria del Consejo Europeo: Conducir la vida como se entiende con un mínimo de injerencias, integridad física y moral, no ser presentado bajo una falsa luz o apariencia, no divulgar sobre hechos embarazosos, protección contra el espionaje y las indiscreciones injustificadas o inadmisibles, protección contra las divulgaciones de informaciones comunicadas o recibidas confidencialmente.

} 1.3.2 INTIMIDAD SEGÚN PROSSER

Según Prosser: Intrusión en la soledad física (hogar, pertenencias, etc), divulgación pública de hechos privados (no deben ser conocidos aunque para los conocidos exista el derecho al olvido), presentación al público de circunstancias personales bajo una falsa luz o apariencia.

[] 1.4 REGLAMENTO UE PROTECCIÓN DE DATOS

} 1.4.1 ARTÍCULO 12 (TRANSPARENCIA DE LA INFORMACIÓN, COMUNICACIÓN Y MODALIDADES DE EJERCICIO DE LOS DERECHOS DEL INTERESADO)

1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios. 4.5.2016 ES Diario Oficial de la Unión Europea L 119/39.
2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.
3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.
4. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.
5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:
a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o
b) negarse a actuar respecto de la solicitud. El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.
6. Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.
7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.
8. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados.

} 1.4.2 ARTÍCULO 13 (INFORMACIÓN QUE DEBERÁ FACILITARSE CUANDO LOS DATOS PERSONALES SE OBTENGAN DEL INTERESADO)

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:
a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; L 119/40 ES Diario Oficial de la Unión Europea 4.5.2016
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.
2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:
a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
d) el derecho a presentar una reclamación ante una autoridad de control;
e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;
f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.
3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.
4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

} 1.4.3 ARTÍCULO 14 (INFORMACIÓN QUE DEBERÁ FACILITARSE CUANDO LOS DATOS PERSONALES NO SE HAYAN OBTENIDO DEL INTERESADO)

Mismo contenido que en el artículo 13, sólo se añade el siguiente punto:

5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:

a) el interesado ya disponga de la información;

b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;

c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o

d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.

} 1.4.4 ARTÍCULO 15 (DERECHO DE ACCESO DEL INTERESADO)

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;

b) las categorías de datos personales de que se trate;

c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;

d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;

e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;

f) el derecho a presentar una reclamación ante una autoridad de control;

g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;

h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.

3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.

} 1.4.5 ARTÍCULO 16 (DERECHO DE RECTIFICACIÓN)

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le concierne. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

} 1.4.6 ARTÍCULO 17 (DERECHO DE SUPRESIÓN O DERECHO AL OLVIDO)

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le concierne, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:
a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; 4.5.2016 ES Diario Oficial de la Unión Europea L 119/43
b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;
c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;
d) los datos personales hayan sido tratados ilícitamente;
e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.
2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.
3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:
a) para ejercer el derecho a la libertad de expresión e información;
b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;
c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;
d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o
e) para la formulación, el ejercicio o la defensa de reclamaciones.

} 1.4.7 ARTÍCULO 18 (DERECHO A LA LIMITACIÓN DEL TRATAMIENTO)

1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:
a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;
b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;
c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;
d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.
2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos sólo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro. L 119/44 ES Diario Oficial de la Unión Europea 4.5.2016
3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

[] 1.5 LEY DE PROTECCIÓN DE DATOS DE 2018

} 1.5.1 ARTÍCULO 28 (OBLIGACIONES GENERALES DEL RESPONSABLE Y ENCARGADO DEL TRATAMIENTO)

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.
2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:
a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.
b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.
c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.
d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.
e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.
f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.
g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.
h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

} 1.5.2 ARTÍCULO 33 (ENCARGADO DEL TRATAMIENTO)

1. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.
2. Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público. Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.
3. El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado. No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.
4. El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.
5. En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

[] TEMAS 3 Y 4:

[] 2.1 PRIMER PUNTO DE DISCUSIÓN SOBRE CÓDIGOS DEONTOLÓGICOS

Deontología: Es lo que hay que cumplir para trabajar de una forma ética y correcta y para evitar crisis sociales en el futuro. Normalmente esta reglamentación surge en los Colegios Profesionales (normas autónomas) o de organismos públicos y/o privados (normas heterónomas).
Código ético de los ingenieros informáticos: Este código se justifica en la medida en que el impacto de la ingeniería tiene doble dimensión (La ética profesional en la consecución de productos, servicios y actividades informáticas y las implicaciones éticas derivadas de su uso). Se tienen tres puntos principales:
Deben existir códigos deontológicos: Éstos deben concebirse de un modo reflexivo que permita efectuar ajustes individuales caso por caso para evaluar comportamientos en determinadas situaciones y tomar decisiones en base a una jerarquía de valores preestablecidos (la existencia de uno no debe reemplazar la necesidad de abordar los principales retos jurídicos en este ámbito sino que ha de complementar esto de diferentes formas). Este código tiene como objetivo secundario introducir un procedimiento para la resolución de los dilemas éticos y permitir que este ámbito funcione de una manera ética y responsable.
Toma de decisiones junto con IA: Las decisiones que implican una inteligencia artificial incidirán sobre las decisiones particulares y de las autoridades administrativas y judiciales ya que es necesario integrar salvaguardias y la posibilidad de control y verificación por parte de las personas en los procesos de toma de decisiones automatizadas.
Seguridad: Debemos tener en cuenta y respetar la integridad física, seguridad, salud y derechos de las personas, además de defenderlos.
Reversibilidad: Es necesario para que haya un control sobre los robots y nunca dejen de actuar de manera segura y estable.

[] 2.2 CÓDIGO ÉTICO INGENIEROS ROBÓTICA UE

Código ético IRUE: Invita a todos los investigadores y diseñadores a actuar de forma responsable y respetando siempre la dignidad, intimidad y seguridad de las personas. Se pide la unión de todas sus disciplinas para que la investigación en robótica sea segura, ética y eficaz. Esto se hace para evitar ciertas consecuencias futuras, cubriendo todas las actividades y desarrollo de esta ciencia. Se tienen cuatro principios que hay que respetar:
Beneficencia: Los robots deben actuar en beneficio del hombre.
Principio de no perjuicio o maleficencia: Los robots no deben hacer daño ni perjudicar a las personas.
Autonomía: La capacidad de tomar una decisión con conocimiento de causa e independiente sobre los términos de interacción con robots.
Justicia: La distribución justa de los beneficios asociados a la robótica y la asequibilidad de los robots usados en el ámbito sanitario.
Derechos fundamentales: Las actividades de investigación en esta materia deben respetar los derechos fundamentales, siempre hay que respetar la dignidad y las autonomías humanas.
Precaución: Siempre debemos tener precaución de nuestros proyectos, anticipándose a los posibles impactos de los resultados que se obtengan.
Participación: Los ingenieros en robótica garantizan la transparencia y el respeto al derecho legítimo de acceso a la información de todas las partes interesadas (hay que tomar las decisiones necesarias).
Rendición de cuentas: Se deben rendir cuentas de impactos sociales y medioambientales de sus investigadores.
Privacidad: Hay que respetar el derecho a la intimidad, la información privada permanecerá privada siempre y hay que hacer cosas en las que se pueda confiar.
Maximizar beneficios y reducir daños: En caso de daños tomar medidas sólidas, y no debe haber mucho riesgo de todos modos.

[] 2.3 CÓDIGO DEONTOLÓGICO INGENIERÍA INFORMÁTICA

} 2.3.1 PRINCIPIOS DEONTOLÓGICOS UNIVERSALES

Principios deontológicos universales: Son aplicables a cualquier profesión tales como la independencia, desinterés, dignidad, obligación de decir la verdad, legalidad y deber de guardar un secreto profesional. Un profesional destinado al servicio de los demás ha de ser ante todo una persona independiente, honrada, leal, honesta y responsable. Asimismo, debe ser especialmente justo y veraz en todas las afirmaciones, especialmente en las que sean públicas y relativas a aspectos técnicos relacionados con su profesión. Por lo tanto, el Ingeniero en Informática ha de cumplir los citados preceptos en relación a su profesión. Asimismo, debe ser especialmente escrupuloso con el tratamiento y utilización que da a la información que maneja y cumplir el deber de secreto, el cual constituye un derecho y un deber básico de la profesión.

} 2.3.2 RESPONSABILIDAD PROFESIONAL

Alcance de la responsabilidad profesional: La responsabilidad profesional en que puede recaer el Ingeniero en Informática en el desempeño de su cometido profesional es de tres clases:
Penal: Por delitos y faltas que se cometan en el ejercicio de la profesión según las normas penales vigentes.
Civil: Cuando actuando con mala fe (dolo civil), negligencia o impericia inexcusable cause daños en los intereses de un cliente sea del ámbito público o privado (retrasos en la ejecución del trabajo encomendado, actividad inoportuna o inadecuada).
Disciplinaria: Cuando infrinja deberes estatutarios de la profesión o normas de ética profesional.

} 2.3.3 ARTÍCULO 7

Todos los Ingenieros en Informática deben respetar y cumplir los siguientes principios fundamentales (honradez, independencia, lealtad, dignidad, legalidad, intereses del cliente, libertad del cliente, secreto profesional, igualdad y función social, adecuación de la tecnología, formación y perfeccionamiento, libre y leal competencia en el ejercicio de la profesión, remuneración, entidades colegiales, incompatibilidades, respeto a la naturaleza y medio ambiente, trabajo en equipo, responsabilidad civil, investigación y docencia, objeción de conciencia).

} 2.3.4 ARTÍCULO 8

El deber principal del Ingeniero en Informática respecto a este código ético y deontológico de la Ingeniería Informática es conocer, difundir, cumplir y velar por su cumplimiento.
El ingeniero en informática debe conocer las sanciones (civiles, penales y deontológicas) en las que pudiera incurrir si incumple sus obligaciones, alcance y responsabilidad profesional, legislación y estándares aplicables.
El Ingeniero en Informática debe cumplir leyes nacionales, reglamentos y regulaciones, convenciones internacionales, normas de organización, código deontológico de su colegio/asociación y los legítimos contratos y compromisos adquiridos.
En relación a la Justicia, el Ingeniero en Informática debe cooperar con la justicia siempre que se lo requiera y denunciar actos fuera de la ley de los que sea testigo y posea pruebas objetivas requeridas por la justicia para demostrar el hecho denunciado.

} 2.3.5 ARTÍCULO 13

El Ingeniero en Informática está obligado, en relación con el secreto profesional, a sujetarse al secreto profesional, como depositario que es de información confidencial, que constituirá un derecho y una obligación de la profesión y que deberá ser respetado incluso después de haber finalizado la prestación de sus servicios, debiendo ser escrupuloso en el cumplimiento de la legislación vigente; no revelar datos o informaciones de carácter reservado o privado que procedan de un cliente y que haya obtenido por razón de su profesión; hacer respetar el secreto profesional a su personal y a cualquier persona que colabore con él en su actividad profesional de forma directa o indirecta, haciendo extensible esta obligación de secreto profesional en la misma forma en que el Ingeniero está obligado, incluso después de haber terminado la relación laboral; únicamente quedarán dispensados de guardar el secreto profesional, previa autorización del presidente de CCII, aquellos ingenieros que se encuentren en alguna de las siguientes situaciones (dispensa de esta obligación por los titulares de la información o autorizados expresamente por éstos para su divulgación; necesidad de divulgación para evitar un daño propio o de un tercero. En cualquier caso, el deber de secreto continuará siendo aplicable respecto de aquella información cuya divulgación no impida la lesión; existencia de una ley que autorice la cesión o comunicación de la información a terceros; existencia de un requerimiento, mandato u orden de autoridad administrativa o judicial que resulte de obligado cumplimiento); el Ingeniero en Informática que se vea perturbado en el mantenimiento del secreto profesional deberá comunicarlo a la Junta de Gobierno del Colegio.

} 2.3.6 ARTÍCULO 16

El Ingeniero en Informática está obligado, en relación con la sociedad, a actuar teniendo como objetivo el servicio a la sociedad, promoviendo en la propuesta de soluciones el bienestar público, social y medioambiental; reconocer los derechos de terceros, patentes y cumplir con la normativa vigente sobre derechos de autor y propiedad intelectual; tratar a todo el mundo con justicia y nobleza, sin discriminar a nadie por razón de nacimiento, raza, sexo, religión, opinión, especialidad o cualquier otra condición o circunstancia de tipo social o personal; promover la Ingeniería Informática como esa rama del conocimiento cuyos logros se encuentran presentes en muchas actividades de la vida cotidiana; no permitir la utilización fraudulenta de su titulación por personas que ilegítimamente llevan a cabo actuaciones profesionales correspondientes a un Ingeniero en Informática, denunciando ante los Organismos Colegiales cualquier tipo de intrusismo profesional que llegue a su conocimiento; ejercer en todo momento su profesión con el máximo rigor, responsabilidad e imparcialidad; dar el visto bueno a los proyectos sólo si cumplen las especificaciones y no atentan contra la calidad de vida, la confidencialidad ni el medio ambiente, con absoluto respeto a los intereses públicos o incluso privados que pudieran resultar afectados; informar puntualmente a las personas interesadas y/o las autoridades competentes sobre cualquier peligro potencial o real para la integridad de las personas y la Sociedad, que considere puedan devenir del software, los sistemas informáticos o los proyectos relacionados; informar acerca de cualquier práctica entre cuyos fines esté la comisión de un delito, en especial si se trata de un delito informático.

} 2.3.7 ARTÍCULO 17

El Ingeniero en Informática está obligado, en relación con proyectos en que interviene, a impulsar la máxima calidad a un coste aceptable y en un plazo razonable, garantizando que quedan claros los compromisos adquiridos, aceptados previamente por el promotor y el cliente; documentar adecuadamente las especificaciones del proyecto sobre el que trabaja, asegurándose que satisfacen los requisitos del usuario y tienen las aprobaciones adecuadas; analizar las consecuencias éticas, económicas, culturales, legales y medioambientales derivadas de cualquier proyecto en el que esté trabajando, aceptando que las conclusiones de dichos análisis podrían llevar a la remodelación del mismo; realizar estimaciones realistas en cuanto a coste, plazo, recursos y resultados de los proyectos, determinando los aspectos de incertidumbre o riesgo que podrían desviar dichas estimaciones; realizar las pruebas y revisiones del proyecto adecuadas, así como de la documentación en la que trabaje; desarrollar los proyectos y la documentación respetando la confidencialidad de aquellos que van a ser afectados por la realización de su trabajo; no efectuar ni aceptar ningún pago o servicio de valor distinto al libremente pactado; rehusar comprometerse en trabajos que crea no sean beneficiosos para sus clientes.

[] TEMAS 5 Y 6:

[] 3.1 CONSIDERACIONES ÉTICAS DE LA INTELIGENCIA ARTIFICIAL

} 3.1.1 ÉTICA Y TÉCNICA

El verdadero Siglo XXI comienza, pues, con el despegue de la I.A. y su generalización y extensión en nuestra sociedad. La Inteligencia Artificial ha supuesto esa línea que separa dos épocas. Está suponiendo una revolución tan importante para el ser humano como lo fue la rueda, la escritura, la revolución francesa o el descubrimiento de la electricidad o de la penicilina.

Detrás de todo proceso dinamizador, de toda revolución debe haber una implicación ética -y su consecuencia jurídica-, porque sus efectos sobre el hombre y su civilización, deben ser beneficiosos y contribuir a una sociedad más justa, con más bienestar. Es decir, toda técnica requiere una ética. La ética debe acompasar el avance científico para impedir que la revolución tecnológica allane al individuo, a la persona y su dignidad humana pese a que queremos que la Inteligencia Artificial tenga un uso ético, puede ocurrir que la utilicemos peligrosamente, O que “avancemos” dejando a la ética “atrás” o “al margen”.

Los ciudadanos sólo tienen dos armas para defenderse de posibles amenazas en su parcela personal. El arma del Derecho y el arma de la ética. Por supuesto que las democracias occidentales tienen en sus Ordenamientos Jurídicos límites al abuso de poder, a la extralimitación de cualquier índole, ya provenga de la propia Administración Pública o de empresas o particulares. Evitar dicha extralimitación debe hacerse tanto con normas autónomas (regulación ética por los propios productores y usuarios de I.A. o de organismos o asociaciones en las que se integren) como con normas heterónomas, dimanantes del Derecho, en este último caso, con la garantía del último de sus resortes que es el Poder Judicial.

} 3.1.2 EL ARMA DE LA ÉTICA

Cuando hablamos de “ética” debemos tener presente que realmente son diversas y variadas, por lo tanto más bien debemos hablar de “éticas”. Deben estar dirigidas hacia el bien, tratar de orientar al individuo a que realice siempre "lo bueno", lo que es moralmente positivo, elegir lo razonable sobre lo irrazonable, el bien sobre el mal.

Dentro de lo que consideramos I.A. hay aspectos que no nos plantean problemas éticos, tan sólo problemas relativos, en su caso, a responsabilidad civil. Efectivamente, dentro de la IA hay aspectos que no nos crean especialmente problemas éticos, muy al contrario, han facilitado nuestra calidad de vida, abaratado costes de servicios, y posibilitado avances tecnológicos con los que estamos encantados. Además, no colisionan especialmente con ningún principio ético importante.

} 3.1.3 ¿QUÉ ES LA IA?

En contraste la I.A. es una tecnología invisible, básicamente software, consiste en la simulación de procesos de inteligencia humana por parte de máquinas, especialmente sistemas informáticos, incluyen el aprendizaje, la función de adquisición de reglas para el uso de la información y razonamiento, usando las reglas para llegar a conclusiones y la autocorrección, todo esto suponen “técnicas” nuevas y desconocidas antes del nacimiento de la I.A.

Es fundamentalmente software. Efectivamente, el software de la robótica, o de los procesos de producción automatizados. Son Programas informáticos avanzados, no se trata de una superinteligencia, sino más bien de un programa que hace algo en concreto. Lo hace muy bien, muchas veces mejor que un humano, de una manera más exacta, pero no llega a tener la capacidad de interrelación que tenemos los humanos.

“machine learning” (introducción de datos estadísticos para que las maquinas aprendan). Se trata de plataformas que contienen algoritmos -procesos- que permiten “aprender” a las máquinas. Lo que hacen es entrenar a la máquina para que considere todas las variables, por lo que se introducen multitud de datos que sean relevantes para conseguir lo que se pretende.

} 3.1.4 ¿REEMPLAZARÁN AL SER HUMANO LOS ROBOTS DOTADOS DE IA?

Es más, parece que ayudan a una vida mejor. Gracias a la I.A. podemos mejorar en medicina, luchar contra las epidemias, contra las enfermedades crónicas, luchar contra el cambio climático, las técnicas de I.A. son absolutamente necesarias. Pero todavía no tienen la aptitud del humano para manejar datos de manera asociativa/intuitiva, son tecnologías específicas. La capacidad asociativa no es autónoma, como la humana, sino fruto de una reiteración y aprendizaje de millones de imágenes, por ejemplo. Los humanos situamos resultados específicos en un conjunto más amplio. Los algoritmos no tienen la panorámica de la mente humana, si bien es verdad que está en continua evolución y desconocemos hasta donde podrán llegar. Puede tener un uso militar tremendamente peligroso para el ser humano.

} 3.1.5 ¿DÓNDE SE ESTÁ DESARROLLANDO LA IA?

Básicamente en empresas tecnológicas punta tales como Google, Apple, IBM, Microsoft, Nvidia, Baidu, y un largo etcétera, todas ellas compañías de una proyección de futuro inimaginable y que cambiarán notablemente nuestro modo de vida. La investigación sólo en pequeña medida se está desarrollando por las Universidades. Obviamente las empresas y corporaciones pagan mucho mejor y que además ofrecen el atractivo de acceder a una tecnología puntera, si bien las Universidades y las O.N.G. no quieren quedarse al margen y están llevando a cabo una loable actuación en el desarrollo de la ética de la I.A.

Dentro de las consideraciones éticas respecto de la Inteligencia Artificial debo destacar:

1. Debe poner en manos de todos los potenciales usuarios mejoras y avances tecnológicos que faciliten su vida, sin distinción de razas o clase social. En pié de igualdad.
2. Debe establecerse un Código de Conducta y Comités de Ética dentro de los centros de investigación. Igualmente deben fomentarse las Agencias Internacionales tanto a nivel intergubernamental como No Gubernamental que fomenten la reflexión ética y jurídica de las nuevas tecnologías que utilicen Inteligencia Artificial.
3. Necesidad de control humano y sometimiento al Derecho en todo momento, que sean los humanos quienes decidan qué pueden hacer o no los robots y hasta donde llevar la I.A.
4. Toda la investigación y desarrollo de la I.A. debe estar caracterizada por la transparencia, la reversibilidad y la trazabilidad y cooperación interdisciplinar.
5. Debe evitarse la concentración de riqueza y poder en manos de minorías y Estados, a costa de los beneficios o por el monopolio fruto de esta nueva era de robots e I.A.
6. No dañar al ser humano, hasta el punto de desarrollar la objeción de conciencia frente a los robots en su aplicación a los humanos, favoreciendo siempre la igualdad de acceso a estas nuevas tecnologías, evitando la brecha robótica, semejante a la lucha contra la brecha digital.

[] 3.2 PUNTOS DE DISCUSIÓN SOBRE ROBÓTICA PRINCIPIOS 2017

} 3.2.1 ¿VA A INCIDIR LA ROBÓTICA EN EL ÁMBITO LABORAL Y LA EMPLEABILIDAD?

Primer punto: Que durante los últimos doscientos años las cifras de empleo han aumentado de manera continuada gracias al desarrollo tecnológico; que el desarrollo de la robótica y de la inteligencia artificial tiene potencial para transformar el modo de vida y las formas de trabajo, aumentar los niveles de eficiencia, ahorro y seguridad y mejorar la calidad de los servicios, y que se espera que, a corto y medio plazo, la robótica y la inteligencia artificial traigan consigo eficiencia y ahorro, no solo en la producción y el comercio, sino también en ámbitos como el transporte, la asistencia sanitaria, las operaciones de salvamento, la educación y la agricultura, permitiendo que los seres humanos dejen de exponerse a condiciones peligrosas, como, por ejemplo, las que entraña la limpieza de lugares contaminados con sustancias tóxicas.
Segundo punto: La robótica y la inteligencia artificial pueden entrañar una transformación del mercado de trabajo y por ello incidirá sobre el futuro de la educación, el empleo y las políticas sociales, de tal manera que todas ellas sean modificarse para adaptarse a los nuevos requerimientos tecnológicos;
Tercer punto: Que, si bien es posible que el uso generalizado de robots no acarree automáticamente la sustitución de puestos de trabajo, sí que es probable que los empleos menos cualificados en sectores intensivos en mano de obra sean más vulnerables a la automatización; que esta tendencia podría devolver procesos de producción a la Unión; que la investigación ha demostrado que el crecimiento del empleo es considerablemente más rápido en los puestos de trabajo que hacen un mayor uso de la informática; que la automatización de los puestos de trabajo puede liberar a las personas de tareas manuales monótonas y permitirles que se dediquen a otras más creativas y significativas; que la automatización obliga a los Gobiernos a invertir en educación y a acometer otras reformas con el fin de mejorar la redistribución en los tipos de capacidades que necesitarán los trabajadores en el futuro.
Cuarto punto: Que debe aclararse la responsabilidad jurídica desde el punto de vista del modelo de empresa y de la definición de las tareas de los trabajadores, en caso de que se produzca una emergencia u otras circunstancias críticas;

} 3.2.2 ¿VAN A INCIDIR LA ROBÓTICA Y LA IA EN EL ÁMBITO SOCIAL Y POLÍTICO?

A la vista de las crecientes fracturas sociales y el declive de la clase media, conviene tener en cuenta que el progreso de la robótica podría traducirse en una elevada concentración de la riqueza y el poder en manos de una minoría.

[] 3.3 REGLAMENTO EUROPEO INTELIGENCIA ARTIFICIAL

} 3.3.1 ARTÍCULO 5

1. Estarán prohibidas las siguientes prácticas de inteligencia artificial:
a) La introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que trascienden la conciencia de una persona para alterar de manera sustancial su comportamiento de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra.
b) La introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que aproveche alguna de las vulnerabilidades de un grupo específico de personas debido a su edad o discapacidad física o mental para alterar de manera sustancial el comportamiento de una persona que pertenezca a dicho grupo de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra.
c) La introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA por parte de las autoridades públicas o en su representación con el fin de evaluar o clasificar la fiabilidad de personas físicas durante un período determinado de tiempo atendiendo a su conducta social o a características personales o de su personalidad conocidas o predichas, de forma que la clasificación social resultante provoque una o varias de las situaciones siguientes:
i) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos enteros en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente;
ii) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos enteros que es injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este.

d) El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:
i) la búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos;
ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista;
iii) la detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido alguno de los delitos mencionados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI del Consejo, para el que la normativa en vigor en el Estado miembro implicado imponga una pena o una medida de seguridad privativas de libertad cuya duración máxima sea al menos de tres años, según determine el Derecho de dicho Estado miembro.
2. El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley para conseguir cualquiera de los objetivos mencionados en el apartado 1, letra d), tendrá en cuenta los siguientes aspectos:
a) la naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema;
b) las consecuencias que utilizar el sistema tendría para los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias.
Además, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley para cualquiera de los objetivos mencionados en el apartado 1, letra d), cumplirá salvaguardias y condiciones necesarias y proporcionadas en relación con el uso, en particular en lo que respecta a las limitaciones temporales, geográficas y personales.
3. Con respecto al apartado 1, letra d), y el apartado 2, cualquier uso concreto de un sistema de identificación biométrica remota «en tiempo real» en un espacio de acceso público con fines de aplicación de la ley estará supeditado a la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente del Estado miembro donde vaya a utilizarse dicho sistema, que la otorgarán previa solicitud motivada y de conformidad con las normas detalladas del Derecho interno mencionadas en el apartado 4. No obstante, en una situación de urgencia debidamente justificada, se podrá empezar a utilizar el sistema antes de obtener la autorización correspondiente, que podrá solicitarse durante el uso o después de este.
La autoridad judicial o administrativa competente únicamente concederá la autorización cuando esté convencida, atendiendo a las pruebas objetivas o a los indicios claros que se le presenten, de que el uso del sistema de identificación biométrica remota «en tiempo real» es necesario y proporcionado para alcanzar alguno de los objetivos que figuran e
n el apartado 1, letra d), el cual se indicará en la solicitud. Al pronunciarse al respecto, la autoridad judicial o administrativa competente tendrá en cuenta los aspectos mencionados en el apartado 2.
4. Los Estados miembros podrán decidir contemplar la posibilidad de autorizar, ya sea total o parcialmente, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley dentro de los límites y en las condiciones que se indican en el apartado 1, letra d), y los apartados 2 y 3. A tal fin, tendrán que establecer en sus respectivos Derechos internos las normas detalladas necesarias aplicables a la solicitud, la concesión y el ejercicio de las autorizaciones a que se refiere el apartado 3, así como a la supervisión de estas. Dichas normas especificarán también para cuáles de los objetivos enumerados en el apartado 1, letra d), y en su caso en relación con cuáles de los delitos indicados en su inciso iii), se podrá autorizar que las autoridades competentes utilicen estos sistemas con fines de aplicación de la ley.

} 3.3.2 ARTÍCULO 6

1. Un sistema de IA se considerará de alto riesgo cuando reúna las dos condiciones que se indican a continuación, con independencia de si se ha introducido en el mercado o se ha puesto en servicio sin estar integrado en los productos que se mencionan en las letras a) y b):

a) el sistema de IA está destinado a ser utilizado como componente de seguridad de uno de los productos contemplados en la legislación de armonización de la Unión que se indica en el anexo II, o es en sí mismo uno de dichos productos;

b) conforme a la legislación de armonización de la Unión que se indica en el anexo II, el producto del que el sistema de IA es componente de seguridad, o el propio sistema de IA como producto, debe someterse a una evaluación de la conformidad realizada por un organismo independiente para su introducción en el mercado o puesta en servicio.

2. Además de los sistemas de IA de alto riesgo mencionados en el apartado 1, también se considerarán de alto riesgo los sistemas de IA que figuran en el anexo III.

[] TEMAS 7 Y 8:

[] 4.1 INTELIGENCIA ARTIFICIAL Y ROBÓTICA (NORMATIVA Y RETOS)

} 4.1.1 LA UNIÓN EUROPEA Y LA INTELIGENCIA ARTIFICIAL

La Comisión propugna un enfoque en tres etapas pero que se solapan entre sí:
1. Establecimiento de los requisitos esenciales para una inteligencia artificial fiable.
2. Lanzamiento de una fase piloto a gran escala para recabar los comentarios de las partes interesadas, proceso en el que estamos inmersos ahora y que detallaré a continuación.
3. Más difícil: búsqueda de un entendimiento universalmente aceptado, un consenso internacional para la inteligencia artificial centrada en el ser humano.

} 4.1.2 CUATRO GRANDES HITOS DE LA UNIÓN EUROPEA

Primer hito: Resolución del Parlamento Europeo, de 16 de febrero de 2.017 con recomendaciones destinadas a la Comisión sobre normas de derecho civil sobre robótica que ya ha quedado obsoleta. Quizás lo más interesante de estas normas fueron las reflexiones sobre el registro de robots inteligentes y los criterios deontológicos para ingenieros de robótica.
Segundo hito: Estrategia europea sobre la inteligencia artificial en abril de 2018, siendo lo más destacable la creación del Grupo de expertos de alto nivel sobre inteligencia artificial, formado por cincuenta y dos expertos independientes que representan al mundo académico, la industria y la sociedad civil y cuyas conclusiones tienen un carácter relevante: «Directrices Éticas para una IA fiable», presentadas el 8 de abril de 2019. Las Directrices éticas para una IA fiable (preparadas por el Grupo Independiente de Expertos de Alto Nivel sobre IA creado por la Comisión Europea en junio de 2018) señalan que los órganos de gestión y los consejos de administración deberían valorar y discutir sobre los sistemas de IA cuando se detecten cuestiones críticas.
Tercer hito: Libro Blanco sobre I.A. (19-II-2020) que supuso un fenómeno de toma de conciencia de la U.E. sobre la importancia de la I.A.
Cuarto hito: Ley de Inteligencia Artificial (Reglamento de 21- IV-2021) es una propuesta de regulación presentada el pasado abril por la Comisión Europea y que tiene como objetivo crear un marco legal para la Inteligencia Artificial. Es una ley que se aplicaría en todos los sectores excepto en el militar y de la que está prevista una reforma próxima de cara a su entrada en vigor. La propuesta de Reglamento Europeo de Inteligencia Artificial, presentada por la Comisión en abril de 2021, propone un marco reglamentario sobre IA con los objetivos de garantizar que los sistemas de IA introducidos y usados en el mercado de la UE sean seguros y respeten la legislación vigente en materia de derechos fundamentales y valores de la Unión; garantizar la seguridad jurídica para facilitar la inversión e innovación en IA, mejorar la gobernanza y los requisitos de seguridad aplicables a los sistemas de IA y facilitar el desarrollo de un mercado único para hacer un uso legal, seguro y fiable de las aplicaciones de IA y evitar la fragmentación del mercado.

} 4.1.3 CREACIÓN DE AGENCIAS Y LEGISLACIÓN SOBRE IA

Voy a mostrar varios ejemplos de cómo el Derecho comienza a acercarse, aunque sea lentamente, a la inteligencia artificial y fijar sus primeras pautas, quizás nuestra primera referencia es la:

1. Así, la Estrategia Nacional de Inteligencia Artificial, de noviembre de 2020, pretende la incorporación de valores humanistas en la Inteligencia Artificial y el desarrollo de una Inteligencia Artificial inclusiva y sostenible, pero no aborda las características que deben tener los algoritmos.
2. Derecho a la protección de datos Con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, toda persona tiene derecho a la protección de los datos de carácter personal que le concierne.
3. La Carta de Derechos Digitales, de julio de 2021, “la Carta no tiene carácter normativo, sino que su objetivo es reconocer los novísimos retos de aplicación e interpretación que la adaptación de los derechos al entorno digital plantea, así como sugerir principios y políticas referidas a ellos en el citado contexto”.
4. Derecho a la identidad en el entorno digital El derecho a la propia identidad es exigible en el entorno digital. Esta identidad vendrá determinada por el nombre y por los demás elementos que la configuran de acuerdo con el ordenamiento jurídico nacional, europeo e internacional, el derecho a la gestión de la propia identidad, sus atributos y acreditaciones. Consecuentemente, la identidad no podrá ser controlada, manipulada o suplantada por terceros contra la voluntad de la persona, deberá garantizarse la posibilidad de acreditar la identidad legal en el entorno digital en todo momento.
5. Derecho al seudónimo siempre y cuando no sea necesaria la identificación personal para el desarrollo de las tareas propias de dicho entorno.
6. Derecho de la persona a no ser localizada y perfilada. El responsable del tratamiento deberá informar explícitamente al interesado sobre la finalidad de la localización, el perfilado o la decisión automatizada y sobre el ejercicio del derecho de oposición, y presentarlos claramente y al margen de cualquier otra información y con pleno respeto al derecho a la protección de datos.
7. Derecho a la ciberseguridad Conforme al ordenamiento jurídico, toda persona tiene derecho a que los sistemas digitales de información que utilice para su actividad personal, profesional o social, o que traten sus datos o le presten servicios, posean las medidas de seguridad adecuadas que permitan garantizar la integridad, confidencialidad, disponibilidad, resiliencia y autenticidad de la información tratada y la disponibilidad de los servicios prestados.
8. Derecho a la herencia digital Conforme a la ley que rige la sucesión, se reconoce el derecho a la herencia digital de todos los bienes y derechos de los que, en el entorno digital, fuera titular la persona fallecida. Corresponde al legislador determinar los bienes y derechos de carácter digital de naturaleza patrimonial transmisibles por herencia y los bienes de la personalidad que pueden ser objeto de defensa, preservación y memoria, así como las personas llamadas, en su caso, a tal función, en defecto de señalamiento por el fallecido.
9. Derechos ante la inteligencia artificial La inteligencia artificial deberá asegurar un enfoque centrado en la persona y su inalienable dignidad, perseguirá el bien común y asegurará cumplir con el principio de no maleficencia.

En el desarrollo y ciclo de vida de los sistemas de inteligencia artificial:

a) Se deberá garantizar el derecho a la no discriminación cualquiera que fuera su origen, causa o naturaleza, en relación con las decisiones, uso de datos y procesos basados en inteligencia artificial.
b) Se establecerán condiciones de transparencia, auditabilidad, explicabilidad, trazabilidad, supervisión humana y gobernanza. En todo caso, la información facilitada deberá ser accesible y comprensible.
c) Deberán garantizarse la accesibilidad, usabilidad y fiabilidad. Las personas tienen derecho a solicitar una supervisión e intervención humana y a impugnar las decisiones automatizadas tomadas por sistemas de inteligencia artificial que produzcan efectos en su esfera personal y patrimonial.

} 4.1.4 ÁMBITO LABORAL

Esas normas son, en primer lugar, en el ámbito laboral, el Real Decreto 688/2021, sobre procedimientos para la imposición de sanciones por infracciones de orden social y para los expedientes liquidatorios de cuotas de la Seguridad Social, la Ley 12/2021, de 28 de septiembre, por la que se modifica el texto refundido de la Ley del Estatuto de los Trabajadores para garantizar los derechos laborales de las personas dedicadas al reparto en el ámbito de plataformas digitales (conocida como Ley Riders), ambas normas tratan de contrarrestar los posibles efectos adversos de los sistemas de Inteligencia Artificial. Si bien todavía no establece un concepto de inteligencia artificial ni se remite a ningún otro texto, sí dice que cuando las administraciones utilicen algoritmos para tomar decisiones, deberán favorecer que los mismos estén dotadas de unos mecanismos (no indicados), que tengan en cuenta criterios de: minimización de sesgos, transparencia y rendición de cuentas. Todo ello siempre que sea factible técnicamente. Además, estos mecanismos deberán incluir también el diseño de los algoritmos, los datos de entrenamiento utilizados por el sistema y cuál es su potencial impacto discriminatorio.
Dice también la ley que las administraciones públicas priorizan la transparencia en el diseño, la implementación y la capacidad de interpretación de las decisiones adoptadas por los algoritmos. Las administraciones públicas, junto a las empresas, promoverán el uso de una inteligencia artificial ética, confiable y respetuosa con los derechos fundamentales. Finalmente, se indica que se promoverá un sello de calidad de los algoritmos.

} 4.1.5 LEY DE IGUALDAD DE TRATO

Contiene la primera regulación positiva del uso de la inteligencia artificial por las administraciones públicas y las empresas en nuestro país.
El contenido del precepto fundamental es el ya famoso Artículo 23. Esta ley se aplicará en los siguientes ámbitos: … o) Inteligencia Artificial y gestión masiva de datos, así como otras esferas de análoga significación criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente. diseño y datos de entrenamiento, y abordarán su potencial impacto discriminatorio. Para lograr este fin, se promoverá la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio. Las administraciones públicas y las empresas promoverán el uso de una Inteligencia Artificial ética, confiable y respetuosa con los derechos fundamentales, siguiendo especialmente las recomendaciones de la Unión Europea en este sentido. Se promoverá un sello de calidad de los algoritmos. Como vemos la I.A. pasa a ser determinante en El nuevo derecho antidiscriminatorio español.
Este artículo 23 va más allá, se sitúa “en el marco de la Estrategia Nacional de Inteligencia Artificial, de la Carta de Derechos Digitales y de las iniciativas europeas en torno a la Inteligencia Artificial”, tres propuestas con un tema común pero muy diferentes enfoques y alcances. el del nuevo art. 23, que elude la referencia al enfoque centrado en la persona, la persecución del bien común y el aseguramiento del principio de no maleficencia.

} 4.1.6 PAPEL DE LA IA EN LOS MODELOS DE GOBERNANZA

La gobernanza de la IA debe integrar componentes de legalidad (no únicamente ha de cumplirse con el Reglamento de IA sino que el uso de la IA debe no infringir el marco legal aplicable), ética y robustez técnica. Estos tres componentes han de implementarse siempre desde el origen, desde el diseño. El cumplimiento con la normativa de IA es una capa añadida a las ya existentes de seguridad de la información, protección de datos personales, de ciberseguridad, etc. El elemento ético incluye una nueva dimensión en los marcos de gobernanza, pues las organizaciones tendrán que rendir cuentas por el espectro ético de las decisiones asociadas al desarrollo, implementación y uso de sistemas de IA. Así, muchas organizaciones están creando códigos éticos para la IA, nombrando responsables de ética en IA e incluso designando paneles, comités o consejos éticos, importando así obligaciones hasta ahora sólo existentes en determinados sectores como el farmacéutico. En definitiva, adicionalmente a la valoración que cada organización debe realizar para cumplir con el futuro reglamento europeo de inteligencia artificial, teniendo en cuenta los importantes beneficios que el uso de la IA entraña para los modelos de negocio de las compañías, resulta esencial que los consejos de administración dediquen tiempo a identificar las oportunidades que el uso de la IA puede conllevar, así como a supervisar la gestión de los riesgos inherentes al uso de esta compleja tecnología. De manera principal, el consejo debe asegurar que las cuestiones éticas están integradas en la estrategia de IA general y plantearse si la estructura de gobernanza de la organización es la adecuada para monitorizar el uso adecuado de la IA.

} 4.1.7 REQUISITOS ESENCIALES PARA LOGRAR UNA IA FIABLE

1. Ya el Grupo de expertos de la Comisión Europea ha extraído una serie de principios de la Carta de Derechos Fundamentales de la UE, destacando cuatro principios: 1 - respeto por la autonomía humana, 2 - prevención de daños, 3 - justicia y 4 - explicabilidad.
2. Por su parte, el Parlamento Europeo propone la creación de una certificación sobre cumplimiento ético de la IA, que sea obligatoria para los sistemas que se desarrollen o utilicen en el territorio de la UE, para orientar a los órganos de administración en la monitorización del cumplimiento de estándares éticos en el uso de la IA.
3. Códigos éticos para la IA, nombrando responsables de ética en IA e incluso designando comités o consejos éticos.
4. Necesidad de que la legislación sea flexible y a prueba de futuras evoluciones de la tecnología. La propuesta de Ley de I.A. es demasiado rígida para poder reaccionar ante una tecnología que se encuentra en un continuo y vertiginoso desarrollo.
5. Minimización de sesgos los conjuntos de datos utilizados “serán pertinentes y representativos, carecerán de errores y estarán completos”, así como que “tendrán las propiedades estadísticas adecuadas”.
6. Transparencia La transparencia de los sistemas algorítmicos, por su parte, se refiere tanto a la información sobre el hecho de que se está utilizando un algoritmo para la toma de decisiones, como el propósito de la herramienta en términos de para qué ha sido diseñada y para qué no; los beneficios clave que se espera que aporte la herramienta algorítmica, así como una justificación ampliada de por qué se utiliza la herramienta y los tipos de métodos o modelos que utiliza el algoritmo. Derecho a una explicación clara e inteligible sobre el funcionamiento y objetivo de los sistemas de IA. La llamada Transparencia. Debe garantizarse la trazabilidad de los sistemas de inteligencia artificial.
7. “¿Reemplazarán al ser humano los robots dotados de I.A.?. La I.A. aplicada a los robots determina que, a largo plazo, la tendencia actual apunta al desarrollo de máquinas inteligentes y autónomas, con capacidad de ser entrenadas para pensar y tomar decisiones de manera independiente, pero ello no solo implica ventajas económicas, sino también distintas preocupaciones relativas a sus efectos directos e indirectos en el conjunto de la sociedad. Es evidente que podrán reemplazar a oficios concretos y determinados, porque el software de la I.A. puede hacer que los robots lo hagan mejor que el ser humano. Por ejemplo en diseño de moda o en proyectos de obra de ingeniería. La precisión del robot no la consigue el ser humano. Pero la creatividad del ser humano nunca podrá ser suplantada. Sí es seguro es que si se mueven dentro de parámetros éticos parece que ayudarán a una vida mejor. Gracias a la I.A. podemos mejorar en medicina, luchar contra las epidemias, contra las enfermedades crónicas, luchar contra el cambio climático. La robótica dotada de I.A. es absolutamente necesaria, de ahí la importancia del factor ético-jurídico. La humanidad se encuentra a las puertas de una era en la que robots, bots, androides y otras formas de inteligencia artificial cada vez más sofisticadas parecen dispuestas a desencadenar una nueva revolución industrial —que probablemente afecte a todos los estratos de la sociedad—, resulta de vital importancia que el legislador pondere las consecuencias jurídicas y éticas, sin obstaculizar con ello la innovación.
8. Sistemas de alto riesgo: Prohibición total del reconocimiento biométrico en espacios públicos, de los sistemas de reconocimiento de emociones y de los sistemas de predicción de delitos. En general se pide una prohibición de todos aquellos sistemas que “plantean un riesgo inaceptable para los derechos fundamentales”.
9. Debe ofrecerse a los individuos herramientas para revertir una situación en la que se vean afectados negativamente por la IA. El Reglamento de I.A. se aparta peligrosamente de la tónica marcada por el Reglamento General de Protección de Datos de 2.016 por la que se dota al ciudadano de una batería de derechos que le permiten defenderse ante 20 posibles abusos como el derecho del ciudadano de ser informado de brechas de seguridad.
10. Derecho a que un sistema de IA de alto riesgo no pueda usar datos de un sujeto.
11. Intervención y supervisión humanas: Los sistemas de inteligencia artificial deben facilitar sociedades equitativas, apoyando la intervención humana y los derechos fundamentales, y no - disminuir, limitar o desorientar la autonomía humana.
12. Robustez y seguridad: La fiabilidad de la inteligencia artificial requiere que los algoritmos sean suficientemente seguros, fiables y sólidos para resolver errores o incoherencias durante todas las fases del ciclo de vida útil de los sistemas de inteligencia artificial.
13. Privacidad y gestión de datos: Los ciudadanos deben tener pleno control sobre sus propios datos, al tiempo que los datos que les conciernen no deben utilizarse para perjudicarles o discriminarlos.

14. Diversidad, no discriminación y equidad: Los sistemas de inteligencia artificial deben tener en cuenta el conjunto de capacidades, competencias y necesidades humanas, y garantizar la accesibilidad.
15. Bienestar social y medioambiental: Los sistemas de inteligencia artificial deben utilizarse para mejorar el cambio social positivo y aumentar la sostenibilidad y la responsabilidad ecológica.
16. Rendición de cuentas: Deben implantarse mecanismos que garanticen la responsabilidad y la rendición de cuentas de los sistemas de inteligencia artificial y de sus resultados. que defina las responsabilidades del personal directivo y de otra índole en relación con todos los aspectos propios de la IA. 21
17. Debe ponerse en manos de todos los potenciales usuarios mejoras y avances tecnológicos que faciliten su vida, sin distinción de razas o clase social. En pié de igualdad. Esto parece que se está consiguiendo pues es comúnmente aceptado que todos tenemos en el bolsillo un teléfono con una tecnología superior a la que está detrás de la primera central nuclear o del primer avión supersónico. Hoy cualquier persona puede aplicar en su vida cotidiana, su negocio, su trabajo, su rutina la I.A. Las empresas tecnológicas obtienen grandes beneficios de la democratización del software a través básicamente de programas informáticos y de los Smartphone. Cualquier avance debe ser al mismo tiempo un avance de la humanidad y beneficiar al mayor número de personas posibles. Se trata de un problema semejante a los avances científicos en medicina y farmacia, muchas veces inaccesible a un número amplio de población, que aunque lo necesita, no tiene medios o dinero para acceder a vacunas, medicinas o tratamientos. Debe fomentarse que se expandan y desarrollen tecnologías que favorezcan la cura de enfermedades, el uso de la I.A. en materia de implantes, exoesqueletos y otras tecnologías capaces de facilitar calidad de vida a personas afectadas por incapacidades físicas, psíquicas o sensoriales. Especialmente mediante el desarrollo de robots asistenciales y robots médicos, funciones asistenciales y rehabilitadoras. Las tecnologías deben ser “más justas”, que favorezcan la lucha contra el hambre, especialmente mediante el desarrollo de la agricultura y ganadería.
18. Necesidad de control humano y sometimiento al Derecho en todo momento, que sean los humanos quienes decidan qué pueden hacer o no los robots y hasta donde llevar la I.A.
19. Debe evitarse a toda costa que esta nueva era de robots e I.A. suponga concentración de riqueza y poder en manos de unas minorías y Estados. Debe darse un impulso adicional a la creación de observatorios conjuntos en materias relacionadas con el Humanismo Tecnológico.
20. No dañar al ser humano, hasta el punto de desarrollar la objeción de conciencia frente a los robots en su aplicación a los humanos, favoreciendo siempre la igualdad de acceso a estas nuevas tecnologías, evitando la brecha robótica, semejante a la lucha contra la brecha digital, o la brecha Norte-Sur. Todos estos retos debemos cumplirlos aunque no genere plusvalías económicas inmediatas. La Inteligencia Artificial debe ayudar a darnos un conocimiento mucho más profundo de la naturaleza del ser humano y solucionar los déficit socioeconómicos que afligen a las sociedades actuales. Como vemos la Inteligencia Artificial nos plantea nuevos horizontes y nuevos retos, como ya he señalado, tanto a la ética como al Derecho si queremos que se mantenga el respeto a la dignidad y a la libertad humana, y ayudará decisivamente a crear sociedades más solidarias tanto en el plano nacional como en el internacional.

[] 4.2 REGISTRO DE ROBOTS, IA Y UE

} 4.2.1 EL DERECHO DE LOS ROBOTS INTELIGENTES

Ya vimos que los requisitos mínimos para poder ser considerados R.I. requerirían, según la Propuesta del Parlamento Europeo:
a) La capacidad de adquirir autonomía mediante sensores y/o mediante el intercambio de datos con su entorno (interconectividad) y el intercambio y análisis de dichos datos.
b) Capacidad de autoaprendizaje a partir de la experiencia y la interacción con su entorno (esto se considera opcional y no necesario en todos los casos).
c) Soporte físico mínimo.
d) Capacidad de adaptar su comportamiento y acciones al entorno.
e) Inexistencia de vida, al menos en el sentido biológico.

} 4.2.2 BASES PARA CONSEGUIR LA PERSONALIDAD ELECTRÓNICA

Para poder abordar este tema debemos tener en cuenta que se trata de cuatro aspectos que podemos estudiarlos separadamente a efectos pedagógicos, pero en la realidad deben darse conjuntamente, unos dependen de otros. Estos son:

1. La personalidad electrónica del Robot Inteligente.
2. El Código Ético de los Ingenieros de Robótica y, por lo tanto, su responsabilidad.
3. El Registro de Robots Inteligentes y sus efectos en materia de responsabilidad de los propios Robots.
4. Diseño y alcance de un Seguro Obligatorio no sólo para que las empresas puedan cubrir los daños causados por sus robots, o para las empresas que diseñan los Robots, sino específico de los individualizados R.I. que puedan cubrir cualesquiera posibles daños.

Los ingenieros de robótica tienen unas exigencias ineludibles cuando construyen un Robot Inteligente, los volvemos a señalar, según establecen las Normas de Derecho Civil U.E. sobre Robótica, se tratan de principios contenidos en la Resolución del Parlamento Europeo y entre las que podemos destacar las siguientes:

a) La reversibilidad y teclas de interrupción de urgencia: La posibilidad de deshacer la última acción o secuencia de acciones de un robot o una IA, que permita al usuario anular las acciones no deseadas o, en caso de emergencia, desconectarlo totalmente. Éste es el famoso “botón rojo” también propuesto por otras entidades y expertos para garantizar que el control último de la inteligencia artificial resida siempre en los humanos.

b) La privacidad: Los individuos no serán personalmente identificables, salvo en caso de consentimiento explícito del afectado, el cual tiene que recabarse antes de cualquier interacción hombre-máquina.

c) La transparencia: Las etapas de toma de decisión del robot inteligente deben ser claras y poder ser objeto de reconstrucción y trazabilidad en todo momento.

d) Seguridad y previsibilidad: La respuesta y ejecución de los robots y de las IA deben realizarse teniendo en cuenta la incertidumbre en la interpretación y en la acción, así como los posibles fallos de los robots o del hombre. La idea es dar un margen de seguridad respecto a la posible falibilidad e imperfecciones de la comunicación humano-máquina.

e) La identificación: El autómata debe ser identificado como tal al relacionarse con humanos. Es decir, en ningún caso, se podrá diseñar un androide o IA que nos engañe al hacerse pasar por un humano. Debemos saber exactamente con qué Robot estamos interactuando.

} 4.2.3 EL REGISTRO DE ROBOTS INTELIGENTES Y LA CREACIÓN DE FONDOS

La personalidad algorítmica será, por lo tanto, una personalidad jurídica independiente de los seres humanos y de las empresas y quedaría reservada solo para los robots avanzados más complejos que interactúen con terceros de forma autónoma e independiente, tal y como ya hemos señalado. Por ende, tal actuación nunca podrá ser atribuida técnica y directamente a un ser humano. Las propuestas del Parlamento Europeo pretenden la creación de un “Registro de Robots de la Unión Europea” y prevé que “la gestión del sistema de registro y de las inscripciones se atribuya a una Agencia de la Unión para la robótica y la inteligencia artificial”. Elemento básico e ineludible será que habrá que ligar a un robot o un grupo de ellos con un fondo económico. Ciertamente Registro, Fondo y R.I. serán tres elementos indisolublemente unidos. El Registro debe asegurar “la asociación entre el robot y el fondo del que depende y que permita que cualquier persona que interactúe con el robot esté al corriente de la naturaleza del fondo, los límites de su responsabilidad en caso de daños materiales, los nombres y las funciones de los participantes y otros datos pertinentes“

} 4.2.4 ROBOTS INTELIGENTES Y LICENCIAS DE USO DE LA INTELIGENCIA ARTIFICIAL

Como intento de solución de todo ello, el Parlamento Europeo ha propuesto en la Resolución que estamos comentando que debe haber un contenido mínimo de la Licencia de Uso de la Inteligencia Artificial, que deberá contemplar, al menos, los derechos y obligaciones para los usuarios de robots inteligentes:

a) El derecho a no temer perjuicio físico ni psicológico.

b) El derecho a esperar que el robot ejecute sus tareas propias, para las que fue diseñado.

c) La obligación de aceptar las limitaciones de percepción, cognición y acción del robot inteligente.

d) La inteligencia artificial deberá respetar la fragilidad y emotividad humana, no generando confusión en cuanto a la realidad de los sentimientos simulados por la máquina.

e) El derecho a la intimidad: el robot deberá respetar la vida privada y, no grabar ni registrar la actividad de los humanos en momentos de privacidad.

f) El no tratar datos de personas sin el consentimiento explícito y previo de las mismas;

g) La obligación de no usar a los robots contra la Ley ni contra la Ética; y

h) En ningún caso, modificar robots para ser usados como armas.

Resumiendo, en su consecuencia, parece necesario y así lo propone la U.E.:

i) La creación de una agencia europea para la robótica y la Inteligencia Artificial;

ii) La posibilidad de la existencia de una definición legal de “robots inteligentes autónomos” junto a un sistema de registro de los más avanzados;

iii) La necesidad de crear un código de conducta consultivo para ingenieros expertos en robótica, dirigido a guiar el diseño ético, la producción y el uso de robots, así como la introducción de valores de responsabilidad social empresarial en la construcción y desarrollo de los mismos, la creación de una nueva estructura de información para las empresas. Ellas deben informar la contribución de la robótica y la Inteligencia Artificial a los resultados económicos, para efectos de impuestos y cotizaciones de seguridad social.

Este sistema sería sólo para los robots avanzados o inteligentes, entendiendo por tales exclusivamente aquellos que tengan capacidad de:

1. adquirir autonomía mediante sensores y/o mediante el intercambio de datos con su entorno (interconectividad) y el análisis de dichos datos,

2. aprender a través de la experiencia y la interacción y adaptar su comportamiento y acciones al entorno.

[] TEMAS 9 Y 10:

[] 5.1 RESPONSABILIDAD CIVIL Y PENAL

1. DELIMITACIÓN RESPONSABILIDAD CIVIL CONTRACTUAL Y EXTRACONTRACTUAL. Art. 1902 Civil. y ss.

De la Lex Aquilia pasando por el art. 1.902 CC. leyes especiales. Responsabilidad contractual y su complemento con la doctrina de la extracontractual. Persona “conocida” y “desconocida”. Acción ilícita – daño – indemnización.

2- RESPONSABILIDAD CIVIL DERIVADA DE DELITO Arts. 116 C.penal. y ss.

Alteración grave del “Orden Público” y que esté “tipificado”. El art. 1.092 CC y 116 C.p.

3- EL ASEGURAMIENTO. El art. 117 C.penal

Leyes de aplicación.

4- REQUISITOS DE LA RESPONSABILIDAD CIVIL PROFESIONAL.

a. El incumplimiento de sus deberes profesionales.
b. La prueba del incumplimiento.
c. La existencia de un daño efectivo.
d. Existencia del nexo de causalidad, valorado con criterios jurídicos de imputación objetiva.
e. Fijación de la indemnización, equivalente:
i. Al daño sufrido (daño emergente)
ii. O proporcional a la pérdida de oportunidades (lucro cesante).

5- LA RESPONSABILIDAD PROFESIONAL.

Los arts. 129 ss. y 197 ss. C.penal; 278 y ss. C.penal

6- RESPONSABILIDAD DEL FABRICANTE O RESPONSABILIDAD DEL ROBOT.

Resolución del Parlamento Europeo 16-febrero-2.017: Responsabilidad (apartados Z, y AA hasta AI)

7- RESPONSABILIDAD DEL EMPRESARIO Y DEL USUARIO DE ROBOT.

El “Robot autónomo inteligente con personalidad jurídica”

8- RÉGIMEN DE LA RESPONSABILIDAD CIVIL DERIVADA DE LA INTELIGENCIA ARTIFICIAL.

a. Proyectos de Reglamentación europea.

[] 5.2 CÓDIGO PENAL 2023

} 5.2.1 ARTÍCULO 116

1. Toda persona criminalmente responsable de un delito lo es también civilmente si del hecho se derivasen daños o perjuicios. Si son dos o más los responsables de un delito los jueces o tribunales señalarán la cuota de que debe responder cada uno.
2. Los autores y los cómplices, cada uno dentro de su respectiva clase, serán responsables solidariamente entre sí por sus cuotas, y subsidiariamente por las correspondientes a los demás responsables. La responsabilidad subsidiaria se hará efectiva: primero, en los bienes de los autores, y después, en los de los cómplices. Tanto en los casos en que se haga efectiva la responsabilidad solidaria como la subsidiaria, quedará a salvo la repetición del que hubiere pagado contra los demás por las cuotas correspondientes a cada uno.
3. La responsabilidad penal de una persona jurídica llevará consigo su responsabilidad civil en los términos establecidos en el artículo 110 de este Código de forma solidaria con las personas físicas que fueren condenadas por los mismos hechos.

} 5.2.2 ARTÍCULO 117

Los aseguradores que hubieren asumido el riesgo de las responsabilidades pecuniarias derivadas del uso o explotación de cualquier bien, empresa, industria o actividad, cuando, como consecuencia de un hecho previsto en este Código, se produzca el evento que determine el riesgo asegurado, serán responsables civiles directos hasta el límite de la indemnización legalmente establecida o convencionalmente pactada, sin perjuicio del derecho de repetición contra quien corresponda.

} 5.2.3 ARTÍCULO 197

Artículo 197.

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, 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. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:

a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o

b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima. Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.

5. 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 una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años.

7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona. Se impondrá la pena de multa de uno a tres meses a quien habiendo recibido las imágenes o grabaciones audiovisuales a las que se refiere el párrafo anterior las difunda, revele o ceda a terceros sin el consentimiento de la persona afectada. En los supuestos de los párrafos anteriores, la pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.

Artículo 197 bis.

1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él 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.

2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

Artículo 197 ter.

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a

terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:
a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o
b) Una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.
Artículo 197 quater.
Si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado.
Artículo 197 quinquies.
Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

} 5.2.4 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 difundieran, revelaran o cedieran 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.

} 5.2.5 ARTÍCULO 280

El que, con conocimiento de su origen ilícito, y sin haber tomado parte en su descubrimiento, realizare alguna de las conductas descritas en los dos artículos anteriores, será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses.

[] 5.3 REGLAMENTO RC IA

} 5.3.1 ARTÍCULO 4 (RESPONSABILIDAD OBJETIVA DE LOS SISTEMAS DE IA DE ALTO RIESGO)

1. El operador de un sistema de IA de alto riesgo será objetivamente responsable de cualquier daño o perjuicio causado por una actividad física o virtual, un dispositivo o un proceso gobernado por dicho sistema de IA.
2. En el anexo al presente Reglamento se enumeran todos los sistemas de IA de alto riesgo y los sectores críticos en los que se utilizan. La Comisión estará facultada para adoptar actos delegados con arreglo al artículo 13 bis para modificar la lista exhaustiva:
a) mediante la inclusión de nuevos tipos de sistemas de IA de alto riesgo y de los sectores críticos en los que se han desplegado;
b) suprimiendo los tipos de sistemas de IA que ya no se considera que presentan un alto riesgo; o
c) modificando los sectores críticos para los sistemas de IA de alto riesgo existentes. Todo acto delegado por el que se modifique el anexo entrará en vigor seis meses después de su adopción. Al determinar la inclusión en el anexo de nuevos sistemas de IA de alto riesgo o sectores críticos mediante actos delegados, la Comisión tendrá plenamente en cuenta los criterios establecidos en el presente Reglamento, en particular los recogidos en el artículo 3, letra c).
3. Los operadores de un sistema de IA de alto riesgo no podrán eludir su responsabilidad civil alegando que actuaron con la diligencia debida o que el daño o perjuicio fue causado por una actividad, un dispositivo o un proceso autónomos gobernados por su sistema de IA. Los operadores no serán responsables si el daño o perjuicio ha sido provocado por un caso de fuerza mayor.
4. El operador final de un sistema de IA de alto riesgo garantizará que las operaciones de dicho sistema de IA estén cubiertas por un seguro de responsabilidad civil adecuado en relación con los importes y el alcance de la indemnización previstos en los artículos 5 y 6 del presente Reglamento. El operador inicial garantizará que sus servicios estén cubiertos por un seguro de responsabilidad empresarial o de responsabilidad civil de productos adecuado en relación con los importes y el alcance de la indemnización previstos en los artículos 5 y 6 del presente Reglamento. Si se considera que los regímenes de seguro obligatorio del operador final o inicial ya vigentes con arreglo a otra legislación de la Unión o nacional o los fondos voluntarios existentes de seguros de empresas cubren el funcionamiento del sistema de IA o el servicio prestado, la obligación de suscribir un seguro en relación con el sistema de IA o el servicio prestado con arreglo al presente Reglamento se considerará cumplida siempre que el correspondiente seguro obligatorio existente o los fondos voluntarios existentes de seguros de empresas cubran los importes y el alcance de la indemnización previstos en los artículos 5 y 6 del presente Reglamento.
5. El presente Reglamento prevalecerá sobre los regímenes nacionales de responsabilidad civil en caso de clasificación divergente por responsabilidad objetiva de los sistemas de IA.

} 5.3.2 ARTÍCULO 5 (IMPORTE DE LA INDEMNIZACIÓN)

1. Un operador de un sistema de IA de alto riesgo que haya sido considerado responsable de un daño o perjuicio con arreglo al presente Reglamento indemnizará:
a) hasta un importe máximo de dos millones de euros en caso de fallecimiento o de daños causados a la salud o a la integridad física de una persona afectada como resultado del funcionamiento de un sistema de IA de alto riesgo;
b) hasta un importe máximo de un millón de euros en caso de daños morales significativos que resulten en una pérdida económica comprobable o en daños a bienes, también cuando distintos bienes propiedad de una persona afectada resulten dañados como resultado de un único funcionamiento de un único sistema de IA de alto riesgo; cuando la persona afectada también disponga de un derecho a reclamar por responsabilidad contractual contra el operador, no se abonará ninguna indemnización en virtud del presente Reglamento si el importe total de los perjuicios materiales o el daño moral es de un valor inferior a [500 euros] .
2. Cuando la indemnización combinada que deba abonarse a varias personas que sufran daños o perjuicios causados por el mismo funcionamiento de un mismo sistema de IA de alto riesgo supere los importes totales máximos previstos en el apartado 1, los importes que deban abonarse a cada persona se reducirán proporcionalmente de forma que la indemnización combinada no supere los importes máximos establecidos en el apartado 1.

} 5.3.3 ARTÍCULO 6 (ALCANCE DE LA INDEMNIZACIÓN)

1. Dentro de los límites para el importe establecidos en el artículo 5, apartado 1, letra a), la indemnización que abonará el operador considerado responsable en caso de daños físicos seguidos de la muerte de la persona afectada se calculará sobre la base de los costes del tratamiento médico que haya seguido la persona afectada antes de su muerte, así como del perjuicio económico sufrido antes del fallecimiento como consecuencia del cese o la reducción de la capacidad de generar ingresos o el aumento de sus necesidades mientras durase el daño antes del fallecimiento. El operador será además responsable de reembolsar los gastos funerarios de la persona afectada fallecida a la parte responsable de sufragar dichos gastos.
Si en el momento del incidente que causó el daño que condujo a su muerte, la persona afectada mantenía una relación con un tercero y tenía la obligación jurídica de asistir a ese tercero, el operador responsable indemnizará al tercero mediante el pago de una pensión alimenticia proporcional a la que la persona afectada se habría visto obligada a pagar, durante un período equivalente a la esperanza de vida media de una persona de su edad y teniendo en cuenta su estado general. El operador también indemnizará al tercero si, en el momento del incidente que provocó la muerte, el tercero había sido concebido, pero todavía no había nacido.
2. Dentro de los límites para el importe establecidos en el artículo 5, apartado 1, letra b), la indemnización que pagará el operador considerado responsable en caso de daño para la salud o para la integridad física de la persona afectada incluirá el reembolso de los gastos del tratamiento médico correspondiente, así como el pago del perjuicio económico sufrido por la persona afectada como consecuencia de la suspensión temporal, la reducción o el cese definitivo de su capacidad de generar ingresos o del aumento consiguiente de sus necesidades acreditado mediante certificado médico.

} 5.3.4 ARTÍCULO 8 (RESPONSABILIDAD SUBJETIVA PARA OTROS SISTEMAS DE IA)

1. El operador de un sistema de IA que no constituya un sistema de IA de alto riesgo, tal y como se define en el artículo 3, letra c), y en el artículo 4, apartado 2, y que, en consecuencia, no figure en el anexo del presente Reglamento, estará sujeto a responsabilidad subjetiva respecto de todo daño o perjuicio causado por una actividad física o virtual, un dispositivo o un proceso gobernados por el sistema de IA.
2. El operador no será responsable si puede demostrar que no tuvo culpa en el daño o perjuicio causado, basándose en uno de los siguientes motivos:
a) el sistema de IA se activó sin su conocimiento, al tiempo que se tomaron todas las medidas razonables y necesarias para evitar dicha activación fuera del control del operador, o
b) se observó la diligencia debida a través de la realización de las siguientes acciones: la selección de un sistema de IA adecuado para las tareas y las capacidades pertinentes, la correcta puesta en funcionamiento del sistema de IA, el control de las actividades y el mantenimiento de la fiabilidad operativa mediante la instalación periódica de todas las actualizaciones disponibles.
El operador no podrá eludir su responsabilidad alegando que el daño o perjuicio fue causado por una actividad, un dispositivo o un proceso autónomos gobernados por su sistema de IA. El operador no será responsable si el daño o perjuicio ha sido provocado por un caso de fuerza mayor.
3. Cuando el daño o perjuicio haya sido causado por un tercero que haya interferido en el sistema de IA por medio de una modificación de su funcionamiento o sus efectos, el operador será, no obstante, responsable del pago de una indemnización en caso de que dicho tercero esté ilocalizable o sea insolvente.
4. A petición del operador o de la persona afectada, el productor de un sistema de IA tendrá la obligación de cooperar con ellos y de facilitarles información en la medida que lo justifique la relevancia de la demanda, a fin de permitir que se determinen las responsabilidades.

[] OTROS RECURSOS:

[] 6.1 CONSTITUCIÓN ESPAÑOLA

} 6.1.1 ARTÍCULO 1

1. España se constituye en un Estado social y democrático de Derecho, que propugna como valores superiores de su ordenamiento jurídico la libertad, la justicia, la igualdad y el pluralismo político.
2. La soberanía nacional reside en el pueblo español, del que emanan los poderes del Estado.
3. La forma política del Estado español es la Monarquía parlamentaria.

} 6.1.2 ARTÍCULO 9

1. Los ciudadanos y los poderes públicos están sujetos a la Constitución y al resto del ordenamiento jurídico.
2. Corresponde a los poderes públicos promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; remover los obstáculos que impidan o dificulten su plenitud y facilitar la participación de todos los ciudadanos en la vida política, económica, cultural y social.
3. 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.

} 6.1.3 ARTÍCULO 10

1. La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social.
2. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España.

} 6.1.4 ARTÍCULO 14

Los españoles son iguales ante la ley, sin que pueda prevalecer discriminación alguna por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social.

} 6.1.5 ARTÍCULOS DEL 15 AL 29

Los artículos del 15 al 29 constituyen la primera sección de los derechos fundamentales y de las libertades públicas.