

RESPONSABILIDAD DIGITAL DEL ESTADO Y BARRERA ÉTICA

Santiago Carretero Sánchez

Profesor Titular de la Universidad Rey Juan Carlos

Académico Correspondiente de la Real Academia de Jurisprudencia y Legislación

CC BY SA ACCESO LIBRE, 2023, URJC, PARA BURJC

RESUMEN

Antes de que nos hayamos percatado, el mundo virtual ha ido acumulando nuestros datos para alcanzar unos objetivos que no siempre conocíamos o preveíamos. Ahora que la digitalización del mundo físico, así como el análisis que permite dicha digitalización, están muy avanzados, tomamos conciencia de su existencia y empezamos a pensar en los efectos, particularmente éticos —y, en consecuencia, jurídicos—, sobre nuestra sociedad. El derecho de la Unión Europea ha dado respuesta a esta cuestión mediante el Reglamento General sobre la Protección de Datos, que entró en vigor en mayo de 2018, propugnando el principio de que la digitalización de los elementos que permiten identificar a una persona física esté condicionada, principalmente, a un consentimiento previo de la persona física con conocimiento de causa

PALABRAS CLAVE

Responsabilidad digital

Teoría de la responsabilidad

Compromiso ético

Nueva culpabilidad

Incumplimiento de las obligaciones

ABSTRACT

Before we know it, the virtual world has been accumulating our data to achieve objectives that we did not always know or foresee. Now that the digitization of the physical world, as well as the analysis that digitization allows, are very advanced, we are becoming aware of its existence and we are beginning to think about the effects, particularly ethical —and, consequently, legal— on our society. The law of the European Union has responded to this question through the General Regulation on Data Protection, which came into force in May 2018, advocating the principle that the digitization of the elements that allow the identification of a natural person is conditioned , mainly, to the prior consent of the natural person with knowledge of the facts.

KEYWORDS

digital responsibility

responsibility theory

ethical commitment

culpability

Breach of ethical obligations

La configuración de un futuro digital de Europa, esto es, una «Europa adaptada a la Era Digital», es una de las prioridades a corto plazo de la Unión Europea. Este camino estratégico hacia la adaptación de la Unión a la Era Digital puede apreciarse no solo en materia de datos, sino también en el ámbito de las tecnologías emergentes como la Inteligencia Artificial. Es hora de preguntarse si este proceso de digitalización- imparable laboral e industrialmente- debe tener límites éticos. Esta evolución se ha venido produciendo en un sector que no es accesible para la gran mayoría de las personas, tanto por su confidencialidad como por su alta tecnicidad.

La fuerza expansiva del Principio general del Derecho de la responsabilidad del Estado se extiende a la responsabilidad digital, pues ese artículo 106.2 de nuestra Constitución garantiza el derecho de los particulares a ser indemnizados por toda lesión que sufran en cualquiera de sus bienes y derechos, salvo en los casos de fuerza mayor, siempre que la lesión sea consecuencia del funcionamiento de los servicios público, en este caso, el mal funcionamiento de los servicios digitales aprobados o implementados o autorizados por el Estado

Antes de que nos hayamos percatado, el mundo virtual ha ido acumulando nuestros datos para alcanzar unos objetivos que no siempre conocíamos o preveíamos. Ahora que la digitalización del mundo físico, así como el análisis que permite dicha digitalización, están muy avanzados, tomamos conciencia de su existencia y empezamos a pensar en los efectos, particularmente éticos —y, en consecuencia, jurídicos—, sobre nuestra sociedad. El derecho de la Unión Europea ha dado respuesta a esta cuestión mediante el Reglamento General sobre la Protección de Datos, que entró en vigor en mayo de 2018, propugnando el principio de que la digitalización de los elementos que permiten identificar a una persona física esté condicionada, principalmente, a un consentimiento previo de la persona física con conocimiento de causa. Los agentes de esta digilitalización son los Estados modernos y las grandes empresas¹. La digitalización y el uso que hacen empresas y Estados de las correlaciones que permite el análisis mediante inteligencia artificial

¹ Las cuestiones éticas en esta materia han sido muy tratadas, en el trabajo de Martínez Martínez, R. “Cuestiones de ética jurídica al abordar proyectos de big data. El contexto general del Reglamento de protección de datos” en la Revista Dilemata, número 24, 2017, pp. 151-164.

son, muchas veces, una omisión de los principios fundamentales del estado de derecho, base de los sistemas jurídicos de las democracias. De manera simplificada, el Estado de derecho se concibe como aquel gobernado por un sistema jurídico en el que toda condena debe fundamentarse sobre una ley preexistente, en el que existe una verdadera tutela judicial — conocimiento de los hechos imputables, fundamentación de la ilicitud, derecho a la defensa y absolución en caso de que un poder judicial independiente no considere la culpa probada—, y en el que la ley, en su sentido amplio, se aplica a todos los individuos y entidades. Recoge, pues, los principios fundamentales del derecho, casi idénticos en todos los sistemas. Hoy en día, el análisis de datos personales y anónimos recogidos por diversas fuentes y cedidos a entidades de todo tipo posibilita que los individuos se puedan ver privados, por ejemplo, del acceso a un seguro, a un crédito o a un puesto de trabajo. Esto nos llevará sin duda, y de nuevo, al problema de la responsabilidad del Estado como persona jurídica y de las empresas igual, por esta invasión a la privacidad. Incluso se intenta un análisis digitalizado y matemático de las soluciones jurídicas que un determinado justiciable tiene cuando acude a un juzgado.

Así, antes de adentrarnos en el Reglamento Data Governance Act (también conocido por sus siglas, «DGA»), parece interesante hacer referencia a la Estrategia Europea de Datos cuyo objetivo no es otro que la Unión Europea lidere una sociedad impulsada por los datos. A través de dicha Estrategia, la Unión Europea está en proceso de configurar un marco legal estructural que ampare el uso de datos, extremo que puede observarse con la Ley de Gobernanza de Datos y la Ley Europea de Datos (más conocida por su denominación en inglés, «Data Act»), ambos reglamentos europeos del Derecho de la Unión.

Esta Estrategia Europea de Datos halla su justificación en que la Unión Europea lidere una sociedad digital impulsada por los datos, pero se sostiene especialmente en las cifras que la Comisión Europea maneja respecto a los datos para 2025. El Reglamento Data Governance Act fue inicialmente propuesto por la Comisión Europea en 2020 y, como se ha señalado en el párrafo anterior, se aprobó el 16 de mayo de 2022. Su entrada en vigor se producirá tras el transcurso de veinte días desde su publicación en el Diario Oficial de la Unión Europea (DOUE) y las nuevas normas que el Reglamento contiene serán de aplicación quince meses después de la entrada en vigor del Reglamento DGA.

Los aspectos más reseñables del señalado Reglamento de Gobernanza de Datos o DGA son los siguientes:

- Se aboga por una mayor reutilización de los datos protegidos del sector público.
- Un nuevo modelo de negocio para la intermediación de datos facilitando, además, la identificación de los proveedores de servicios.
- Cesión altruista de datos en la Unión Europea con el bien común como objetivo².

² Rodríguez, A.G. “La donación de datos como herramienta para la gobernanza digital” en Bie3: Boletín IEEE, número 18, 2020, pp.739-747.

- Creación del European Data Innovation Board.
- Acceso y transferencia internacional de datos no personales³.

En lo que concierne a la apuesta por una mayor reutilización de determinadas categorías de datos protegidos en manos de organismos del sector público, es inevitable mencionar la «Open Data Directive» por la novedad que aporta la norma respecto a lo previsto en dicha Directiva. A la luz del artículo 3 de la DGA, el legislador apuesta por la reutilización de datos relativos a secretos comerciales y profesionales, datos estadísticos confidenciales, datos relativos a la protección de derechos de propiedad intelectual de terceros y datos personales.

Así, mediante este texto legal y a la luz de su artículo 3, se busca apostar por la reutilización de datos relativos a secretos comerciales y profesionales, datos estadísticos confidenciales, datos relativos a la protección de derechos de propiedad intelectual de terceros y datos personales. Ello supone un verdadero cambio y, podría decirse que aporta la mayor novedad, habida cuenta la exclusión de estos datos en el ámbito de aplicación de la precitada Directiva.

En cuanto a la creación de un nuevo modelo de negocio basado en la intermediación de datos, se pretende el intercambio de datos en un entorno seguro a través de la prestación de servicios de intermediación de datos, prestación de servicios que se encuentra sujeta a procedimiento de notificación y a la extensa relación de condiciones expuestas en el artículo 12 del Reglamento DGA.

Una de las condiciones para la prestación de servicios de intermediación de datos que más destaca, y de la cual merece la pena su especial mención, es la relativa a los fines de los datos ya que, de acuerdo con lo previsto en el Reglamento Data Governance Act, «los proveedores de servicios de intermediación de datos no podrán utilizar los datos en relación con los que presten sus servicios para fines diferentes de su puesta en disposición».

El tercer punto clave consiste en la cesión altruista de datos entre los Estados miembros con el bien común o interés general como objetivo, enmarcándose en el bien común aquellos datos relativos —se citan algunos de ellos— a la asistencia sanitaria, lucha contra el cambio climático, mejora de la prestación de servicios públicos, investigación científica de interés general⁴...

³ Domínguez Álvarez, J.L. “El tratamiento ulterior de datos personales con fines archivísticos y la importancia creciente de la reutilización de la información” en la Revista Archivamos: Boletín ACAL, número 118, 2020, pp. 2020, pp. 4-11.

⁴ Merino Gómez, G. “Nuevos desafíos en torno al big data” en Revista de Derecho y genoma humano: genética, biotecnología y medicina avanzada, número 1, (extra, dedicado al uso de datos clínicos ante nuevos escenarios tecnológicos y científicos. Oportunidades e implicaciones jurídicas”, 2019, pp. 37-54.

Esta cesión altruista de datos es de carácter voluntario y se puede realizar, según lo establecido en el Capítulo IV del Reglamento DGA, mediante la cumplimentación de un formulario de consentimiento de altruismo de datos europeos en el que, si se facilitan datos personales, deberá garantizar que se cumpla con las exigencias previstas en el Reglamento General de Protección de Datos.

Otro de los aspectos más reseñables es que, bajo el amparo del Reglamento Data Governance Act, se crea el European Data Innovation Board que adoptará forma de grupo de expertos y estará compuesto por representantes de las autoridades competentes señaladas en el artículo 29.1 del Reglamento DGA —debiendo estar compuesto, como mínimo, por los tres subgrupos previstos en el apartado siguiente del precitado artículo—.

En el artículo 30 del Reglamento DGA se ofrece extensa relación de funciones del European Data Innovation Board, destacando entre estas, el asesoramiento y asistencia a la Comisión Europea para mejorar la interoperabilidad de los servicios de intermediación de datos y la propuesta de directrices para marcos interoperables de normas y prácticas comunes para el procesamiento conjunto de datos para alcanzar los fines descritos en el artículo 30.h) del Reglamento DGA.

Por último, tenemos el acceso y transferencia internacional de datos no personales. Es importante señalar que se protegen los datos del sector público, los servicios de intermediación de datos y las organizaciones de altruismo de datos tanto de las transferencias internacionales ilegal de datos no personales como del acceso gubernamental a estos⁵.

Sin perjuicio de lo anterior, el Reglamento DGA permite la transferencia de datos no personales a terceros países, guardando cierta similitud con el Reglamento General de Protección de Datos (RGPD), mediante la adopción de decisiones de adecuación por las que se declare que determinados terceros países cuentan con medidas de protección similares a las de la Unión Europea o sus Estados miembros. El Reglamento Data Governance Act deja patente que la Unión Europea es consciente del papel clave que juegan los datos en la transformación socioeconómica a la que venimos acudiendo en los últimos tiempos y que, dentro del marco de la Estrategia Europea de Datos, permitirá desarrollar un auténtico espacio común europeo de datos y más productos innovadores a la altura de la Era Digital que la Unión Europea desea, más pronto que tarde, alcanzar. Eso conllevará unos mecanismos más directos en los fallos de compliance, que el propio Estado debe dotarse, y aun cuando el avance en la Unión Europea es realmente tremendo, queda mucho por hacer.

⁵ La transferencia de datos personales a terceros países no debe aun así menoscabar el nivel de protección reconocido en la UE, STJUE, Gran Sala, Sentencia de 16 de julio de 2020, estudio de esta en Actualidad Administrativa, número 9, 2020.

PROBLEMAS CONCRETOS DE LA RESPONSABILIDAD EN LA INTELIGENCIA ARTIFICIAL y SU COMPATIBILIDAD CON LA TEORÍA TRADICIONAL

Estamos ante una petición de responsabilidad exigida a una persona jurídica, Estado o gran empresa de data, que pueden vulnerar gravemente nuestra intimidad. Es por ello, que, aunque estemos hablando del delegado de protección de datos en cada momento, nos deberemos orientar a la responsabilidad penal, siendo esta la más fuerte, de las personas jurídicas, también en sus consecuencias civiles. Asistimos en estos momentos a la aparición de nuevas expectativas jurídicas, nuevos retos que el Derecho no puede desconocer. Algunos pasan desapercibidos, pero desde luego, no puede serlo la primera resolución judicial del Tribunal Supremo español que versa sobre la responsabilidad jurídica de las personas físicas, nos referimos a la importante sentencia 154/2016 de 29 de febrero que declara responsables penales a personas jurídicas. Esto rompe con una teoría sobre la persona jurídica, sobre su capacidad y voluntad para ser merecedora de un reproche penal. Hasta ahora, la responsabilidad penal venía dada por el cargo de la sociedad, por sus representantes legales, y esa misma se extendería sólo a sus bienes, sin perjuicio de que, cuando se cobraban esos bienes desde los societarios, la sociedad pudiera repetir por sus acciones civiles y penales a ese socio. Ese tema estaba claro y no rompía la teoría tradicional de la persona jurídica. Pero el caso es que la resolución de febrero de 2016 ha sido histórica, la primera, que se plantea el tema de la responsabilidad en global, a toda la persona jurídica en sí. Algo que ya permitía nuestro art. 31 bis del CP en sus letras a) y b) que permite transferir la responsabilidad de las personas físicas a las jurídicas. El primer hecho de conexión lo generan las personas con mayores responsabilidades en la entidad y el segundo las personas indebidamente controladas por aquéllas. En aquellos casos, se establece un sistema de responsabilidad por transferencia o vicarial de la persona jurídica, aunque la novedosa regulación de los programas de cumplimiento normativo introducidos por la LO 1/2015 nos acerca un poco más al ambicioso modelo de «culpabilidad por defecto de organización». Indica Legaz que el sujeto de Derecho es el ser que es capaz de derechos y obligaciones. El punto de partida de nuestro Derecho occidental es el hombre, el sujeto de Derecho es el hombre por influencia del cristianismo, de toda la doctrina ética kantiana. No se trata de hacer un repaso de clara Filosofía del Derecho sobre las doctrinas que afirman que las características de inteligencia y voluntad sí son aplicables a asociaciones de personas físicas, como las teorías de Gierke, Del Vecchio, o las teorías idealistas como Binder, Larenz... es clara ya la idea de las teorías patrimonialistas, Mayer como la teoría de la persona jurídica como empresa, o la doctrina del patrimonio colectivo (Planiol), el propio Kelsen considera la persona jurídica dentro del orden jurídico no la ve ficción alguna del Derecho. Eran otros tiempos. Había autores que negaban la existencia de la persona jurídica como tal como Duguit al negar el derecho subjetivo, o Hoelder que no entiende aplicables las características de la persona a la persona jurídica, conocimiento, voluntad, acción. Una mera ficción como indica Affolter. Hoy en Día no tiene sentido, nuestra economía está basada en personas jurídicas, bien institucionales (Estado, Nación) o bien desde el punto de vista mercantil (Sociedad de todas las diferentes formas) es más, cuantas más empresas, personas jurídicas existan, más próspero es un país. Cualquier empresa, por pequeña que sea, en

cuanto aumenta su objeto social, contrata a otros trabajadores, cuando aumenta su producción, difícilmente no adopta forma societaria. Por tanto, el debate sobre la existencia o no de la persona jurídica, nos lleva a un terreno más epistemológico que jurídico, a un planteamiento pre jurídico, que, como tal, hoy en día ya no se puede volver atrás. Desde el Derecho romano, el que hace verdaderamente que exista la persona jurídica, la realidad del Derecho se ha ido institucionalizando, pero, aun así, el concepto persona jurídica era una ficción como se indicaba en el aforismo conocido ya de *societas delinquere non potest*. Y ello ha pasado con la responsabilidad, el proceso de objetivación del daño en el terreno civil se ha observado en el Derecho penal. De ahí que esta resolución sea histórica por sus repercusiones mercantiles, económicas, jurídicas y de reflexión. Por ello, ya nadie pone en duda la existencia de una responsabilidad estatal en este campo, la responsabilidad digital y sus nuevos derechos⁶. El Plan de España Digital 2025, alineado con la Agenda Digital para Europa, hace referencia expresa al derecho a la protección de los datos personales como derecho fundamental en la UE, abriendo un marco de acción en las administraciones públicas, que, basado en el dato seguro y su minimización, impulse la mejora de los servicios públicos digitales. En su reciente Comunicación Brújula digital 2030: el camino europeo para la década digital, la Comisión Europea hace hincapié en una administración pública conectada, así como en la construcción, desde la complementariedad, de un sistema único que permita el intercambio de datos respetando en su plenitud los derechos fundamentales; los de privacidad, protección de datos e intimidad, derecho al olvido y libertad de expresión, entre ellos, incluyendo el acceso a medios plurales, fiables y transparentes de información. La «ciudadanía digital» reclama mayor control de sus datos, mayor transparencia, seguridad y privacidad, porque el mundo de hoy está generando más datos que nunca. Navegación en las webs, redes sociales, telefonía, mails, dispositivos GPS..., gestan, de manera espontánea en su mayoría, un caudal de datos que ocasiona el fenómeno «big data» o «new data», con implicaciones en el mundo del trabajo. El «big data» y, con él, los algoritmos y otros sistemas de inteligencia artificial permiten la observación, seguimiento y control, facilitando los procesos decisorios; también posibilitan la medición de ciertos acontecimientos y la realización de predicciones. El riesgo de que los datos, los algoritmos y los softwares que los sustentan, inicialmente diseñados para usos concretos, sean utilizados con finalidades distintas son amenazas que planean en el universo digital, cuya revolución impacta en las relaciones de trabajo, abarcando un espectro multidimensional cada vez mayor. La vigilancia y gestión del rendimiento, las interacciones entre la oferta y la demanda de trabajo, la obtención de información relativamente detallada sobre las características de las personas trabajadoras y empleadoras, comportan nuevos riesgos que deben ser ampliamente abordados en el plano jurídico, tomando en consideración que los medios actuales de acopio, tratamiento y recuperación de datos revisten cada vez mayor complejidad. Sus formas de utilización y difusión, además de facilitar la vigilancia, permiten influir en las personas trabajadoras y empleadoras, en sus comportamientos y decisiones. Cada vez los juristas se preguntan más dónde encajar la responsabilidad de personas jurídicas que pertenecen al sector de la

⁶ Rallo Lombarte, A. “Una nueva generación de derechos digitales” en la Revista de Estudios Políticos, número 187, 2020, pp. 101-135.

robótica y de la Inteligencia artificial⁷. A este respecto, el Dictamen de 2017 del CESE señala la controversia sobre quién asume la responsabilidad de los daños que pueda causar un sistema de inteligencia artificial, también en el caso de que se trate de sistemas autodidactas que continúan el aprendizaje después de entrar en servicio. El Parlamento indica que es conveniente definir el concepto de «Robot autónomo inteligente» teniendo en cuenta elementos tales como su autonomía, capacidad de autoaprendizaje, soporte, adaptación del comportamiento.

Las consideraciones que realiza el Parlamento Europeo se pueden condensar en las siguientes:

- a) La dotación a los robots de rasgos cognitivos y autónomos, antes propios sólo de los seres humanos. Se asimilan a los agentes interactuantes del entorno y pueden modificarlo, y de ahí la cuestión de la responsabilidad por daños.
- b) Autonomía y capacidad de decisión por parte de los robots con independencia del control. Si hay mayor sofisticación, habrá mayor autonomía⁸.
- c) La mayor autonomía se traduce en la superación de la instrumentalidad del robot, por lo que se plantea si la normativa existente en materia de responsabilidad es adecuada o se precisa normas y principios sobre la responsabilidad jurídica de los agentes (fabricante, operador, propietario, usuario) por los daños y perjuicios de los actos y omisiones de los robots, que no se pueda atribuir a un agente en concreto, y también de los actos y omisiones dañinos que podían evitarse.
- d) La naturaleza jurídica de los robots incluyéndolos dentro de una categoría existente o crear una nueva expresada para ellos.
- e) En el actual marco legal, los robots no son sujetos responsables por daños a terceros. Las normas vigentes contemplan la responsabilidad al agente humano (fabricante, operador, propietario o usuario), tanto en la previsión del daño como en la omisión de este por parte de los robots.
- f) La responsabilidad por daños causados por productos defectuosos en la que el fabricante responde por un mal funcionamiento, y en las que el usuario responde por un mal comportamiento se aplica a los robots.
- g) Si un robot es autónomo en la toma de decisiones, las normas existentes no serán suficientes para generar responsabilidad por los daños, ya que no pueden determinar la parte que deba indemnizar, ni la reparación del daño causado.
- h) Deficiencias en las normas de responsabilidad contractual en el caso de máquinas para elegir parte contractual, celebrar contratos, por lo que es preciso adoptar normas que sean aplicables en un marco tecnológico.

⁷ Ramón Fernández, F. “Robótica, inteligencia artificial y seguridad: ¿cómo encajar la responsabilidad civil?” en el Diario la Ley, número 9365, 2019.

⁸ Lledó Benito, I. “El impacto de la robótica: la inteligencia artificial y la responsabilidad penal en los robots inteligentes” en la Revista Foro Galego, Revista Xuridica, número 208, 2020, pp. 173-202.

i) Insuficiencia de la normativa en materia de responsabilidad extracontractual en el ámbito comunitario, ya que sólo cubre los daños ocasionados por defectos de fabricación de un robot a condición de que el perjudicado pueda demostrar el daño real, el defecto del producto y la relación causa efecto entre el defecto y el daño (responsabilidad objetiva o sin culpa). Inaplicación de la normativa referida para cubrir los daños ocasionados por robots, y teniendo en cuenta sus capacidades e imprevisibilidad en la actuación.

El Parlamento Europeo recomendó el examen de dotar a los robots de personalidad jurídica para atribuirles responsabilidad civil por daños, siendo esto importante para la exigencia de Responsabilidad del Estado también⁹.

El Parlamento Europeo formuló recomendaciones respecto a la legislación civil en materia de robótica, y el examen de dotar a los robots de personalidad jurídica, e-personality, para atribuirles responsabilidad civil por daños.

Ha dictado unos «Principios generales relativos al desarrollo de la robótica y la inteligencia artificial para uso civil»:

1. La responsabilidad por daños y perjuicios causados por robots debe ser analizada para garantizar la eficiencia, transparencia y coherencia en la garantía de la seguridad jurídica en la UE en beneficio de ciudadanos, consumidores y empresas.
2. La importancia de las relaciones de interdependencia básicas, previsibilidad y direccionalidad para determinar la información que compartan humanos y robots.
3. Necesidad de propuesta de legislación sobre los aspectos jurídicos relacionados con el desarrollo y uso de la robótica y la inteligencia artificial¹⁰.
4. La herramienta legislativa para la responsabilidad civil por daños y perjuicios causados por robots en casos diferentes a los perjuicios económicos, no debe limitar el alcance de la responsabilidad patrimonial que pueda ser compensada, ni su naturaleza, por el hecho de que sean causados por un robot.
5. El instrumento legislativo debe basarse en una evaluación para determinar el enfoque de la responsabilidad objetiva o el de gestión de riesgos.
6. La responsabilidad objetiva precisa probar el daño, nexo causal y perjuicios sufridos, pero no la intención, en esto ha ido de la mano de la teoría tradicional de la responsabilidad patrimonial moderna y se tendrán que regular los supuestos de hecho, detrás estará el ser humano siempre.

⁹ Salardi, S. "Robótica e inteligencia artificial: retos para el Derecho" en la Revista Derecho y Libertades: Revista de Filosofía del Derecho y derechos humanos, número 42, 2020, pp. 203-232.

¹⁰ Santos González, M.J. "Regulación de la robótica y la inteligencia artificial: retos de futuro" en la Revista Jurídica de la Universidad de León, número 4, 2017, pp. 25-50.

7. La gestión de riesgos no está centrada en el ámbito subjetivo o actuación negligente, sino en la persona capaz de minimizar riesgos y gestionar el impacto negativo.

8. La identificación de las partes será un elemento para aplicar la responsabilidad proporcionar según las instrucciones que hayan dado las mismas a los robots, y el grado de autonomía de estos. Influirá las capacidades adquiridas y la formación otorgada por el ser humano a la máquina, por lo que no se puede confundir la competencia adquirida por la formación con la competencia dependientes de la capacidad de aprendizaje autónomo.

9. Establecimiento de un régimen de seguro obligatorio similar a los vehículos, pero cubriendo todas las responsabilidades potenciales y no sólo las actuaciones humanas y los fallos mecánicos. Complemento con un fondo para garantizar la reparación de los daños en los casos de ausencia de cobertura del seguro, por lo que habría que generar nuevos productos que se adapten a dichas circunstancias¹¹.

Se solicita a la Comisión que, en la evaluación de impacto de la futura regulación, se consideren las implicaciones de todas las soluciones jurídicas, como las siguientes:

«a) establecer un régimen de seguro obligatorio en los casos en que sea pertinente y necesario para categorías específicas de robots, similar al existente para los automóviles, en el que los fabricantes o los propietarios de robots estarían obligados a suscribir un contrato de seguro por los posibles daños y perjuicios causados por sus robots, no siempre sería el Estado el responsable así.

b). - establecer un fondo de compensación que no sólo garantice la reparación de los daños o perjuicios causados por un robot ante la ausencia de un seguro.

c). - Decidir si conviene crear un fondo general para todos los robots autónomos inteligentes o crear un fondo individual para cada categoría de robot, así como la elección entre un canon único al introducir el robot en el mercado o pagos periódicos durante la vida del robot.

d) crear un número de matrícula individual que figure en un registro específico de la Unión que asegure 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.

e). - crear a largo plazo una personalidad jurídica específica para los robots, de forma que como mínimo los robots autónomos más complejos puedan ser considerados personas electrónicas responsables de reparar los daños que puedan

¹¹ Martínez Muñoz, M; Veiga Copo, A. *Retos y desafíos del contrato de seguro: del necesario aggiornamento a la metamorfosis*. Pamplona: Aranzadi. Dentro de esta obra el artículo de Badillo Arias, "La Responsabilidad civil y el aseguramiento de los robots", pp. 913-954.

causar, y posiblemente aplicar la personalidad electrónica a aquellos supuestos en los que los robots tomen decisiones autónomas inteligentes o interactúen con terceros de forma independiente»¹².

Por su parte, la Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Inteligencia artificial para Europa (COM/2018/237 final), establece respecto a la responsabilidad por daños:

«La aparición de la IA, en particular el complejo ecosistema que la hace posible y la característica de la adopción autónoma de decisiones, exige una reflexión acerca de la idoneidad de algunas de las normas establecidas en materia de seguridad y de cuestiones de Derecho civil relativas a la responsabilidad.

Por ejemplo, los robots avanzados y los productos del internet de las cosas que se apoyan en la IA pueden no comportarse con arreglo a lo previsto cuando el sistema entró en funcionamiento por primera vez. Habida cuenta de la generalización de la utilización de la IA, es posible que sea necesario revisar las normas tanto horizontales como sectoriales.

El marco de seguridad de la UE ya se ocupa de la cuestión del uso previsto y del uso (o abuso) previsible de los productos cuando se comercializan. A raíz de ello, se ha elaborado un sólido conjunto de normas para los dispositivos que se apoyan en la IA, normas que se adaptan constantemente en consonancia con el progreso tecnológico.

La transferencia de responsabilidad civil al robot, al tener la normativa sobre responsabilidad un efecto de carácter preventivo o cautelar y correctivo, supondría la desaparición de esa nota. El otorgamiento de responsabilidad jurídica podría ser susceptible de un uso y aplicación indebido. No es válido compararla con la responsabilidad limitada societaria, ya que al final el responsable es una persona física. Habrá que atender también a cómo se contempla en la legislación de cada Estado la responsabilidad por producto defectuoso (entendiéndose como producto cualquier bien mueble, aun cuando esté incorporado a otro bien mueble o inmueble), teniendo en cuenta, por ejemplo, la Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos, modificada por Directiva 1999/34/CE del Parlamento Europeo y del Consejo, de 10 de mayo de 1999, y en el caso de España, se atenderá a lo indicado en el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes

¹² García-Antón Palacios, E (dir). *Los derechos humanos en la inteligencia artificial: su integración en los ODS de la Agenda 2030*. Pamplona: Thompson-Aranzadi, 2022. Dentro de esta obra hay que destacar el trabajo de Goñi Huarte, E. “La personalidad jurídica de los robots” pp.293-314.

complementarias, modificado por Ley 3/2014, de 27 de marzo, y Ley 4/2018, de 11 de junio.

Dentro de la categoría de los robots, la doctrina se refiere como agentes morales (implícitos, explícitos y plenos) a los que son capaces de tomar decisiones de trascendencia moral y jurídica, dado su grado de autonomía y complejidad, que los lleva a adoptar un comportamiento no del todo previsible. Se caracterizan con las notas de interactividad, autonomía y adaptabilidad. Dentro de ellos, nos podemos encontrar con los denominados automóviles autónomos, los robots quirúrgicos y asistenciales, los drones, o cualquier tipo de inteligencia artificial capaz de crear una obra original, que plantearía cómo resolver los derechos de autor), cuestión esta última que no se contempla en el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia, modificado por Real Decreto-ley 12/2007, de 3 de julio, y Real Decreto-ley 2/2018, de 13 de abril.

Respecto a los drones, el Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea, en su art. 26, indica que se dispondrá de una póliza de seguro u otra garantía financiera para cubrir la responsabilidad civil a terceros por daños, estamos viendo en la guerra de Ucrania ser instrumento bélico para los ataques de Estado¹³.

Junto a ello hay que tener en cuenta lo dispuesto en la Resolución de 2 de marzo de 2018, de la Dirección de la Agencia Estatal de Seguridad Aérea, por la que se adoptan los medios aceptables de cumplimiento y material guía, aprobados para las operaciones con aeronaves pilotadas por control remoto, en virtud de la Disposición Final Cuarta del Real Decreto 1036/2017 de 15 de diciembre.

En el reciente Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo de 4 de julio de 2018 sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de la Unión Europea para la Seguridad Aérea y por el que se modifican los Reglamentos (CE) n.o. 2111/2005 (CE) n.o. 1008/2008 (UE)n.o. 996/2010 (CE)n.o. 376/2014 y las Directivas 2014/30/UE y 2014/53/UE del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) n.o. 552/2004 y (CE) n.o. 216/2008 del Parlamento Europeo y del Consejo y el Reglamento (CEE) n.o. 3922/91 del Consejo, en su Anexo VI referente a los requisitos esenciales de los organismos cualificados se indica que éste deberá

¹³ Badouin, L. "Overview of The French and European Regulations On Aerial Drone" en la revista ecuatoriana Foro: Revista de Derecho, números 36 y 35, pp. 73-90.

contratar un seguro de responsabilidad civil, salvo que un Estado miembro asuma dicha responsabilidad según su Derecho interno.

Se menciona también la responsabilidad extracontractual que cuyos daños serán reparados por la Agencia o su personal, según la aplicación de los principios generales comunes al Derecho de los Estados miembros.

Con la legislación actual, la imputación de responsabilidad a la máquina o robot no es posible, ya que siempre es una persona quien asume la responsabilidad, sea el fabricante, dueño o usuario. Siguiendo el sistema de responsabilidad objetiva, existencia del daño, y no en la culpa, como sucede en la responsabilidad subjetiva. En la legislación española se opta por la primera, por la aplicación de la legislación anteriormente indicada de consumidores y usuarios. No puede desaparecer la responsabilidad personal en esta materia tampoco. La causa del daño está relacionada con la responsabilidad y quién asume la misma. En el caso de las máquinas se debe relacionar la inteligencia artificial de la que está dotada y el aprendizaje del aparato, cuanto mayor sea su autonomía en la capacidad de realizar una tarea a través del aprendizaje, mayor será la responsabilidad de la máquina; y, al contrario, si se aumenta la dependencia humana, la responsabilidad disminuirá en la máquina. En verdad, nos encontraríamos ante la denominada probatio diabólica si se optara por el sistema de culpa, por lo que la responsabilidad objetiva, daño y responsabilidad con independencia de la intención, será el más idóneo para obtener el resarcimiento, realmente no quedará otra posibilidad. A ello irá unido la contemplación del riesgo y su cobertura en materia de seguros que deberá de suscribir el fabricante de la máquina para asumir su responsabilidad civil¹⁴.

PRINCIPIOS GENERALES Y NUEVA CULPABILIDAD

Se plantea el problema más que de culpabilidad de la delimitación de esa responsabilidad. Porque cualquier ejecución de una decisión empresarial pasa por muchas cabezas pensantes, por muchos agentes. Si bien es cierto que la implementación de las medidas es una acción empresarial conjunta la puesta en funcionamiento también lo es. La cadena de responsabilidad es lo que hay que determinar, porque esa responsabilidad puede residir en el órgano de control de la supervisión, la vigilancia de que ese protocolo se aplique. En el caso de esta sentencia histórica la existencia de una organización criminal que operaba a través de tres sociedades mercantiles dedicadas a la exportación e importación de maquinaria, en la que se llegaron a ocultar más de 6000 kg de cocaína en su interior, que hubiera alcanzado un valor superior a los 250 millones de euros de haber ingresado en el mercado. Aplicada la doctrina anterior, el TS confirma la responsabilidad penal ex art. 31 bis declarada por la Audiencia nacional respecto de dichas empresas, utilizadas para traficar con droga. En el Estado una decisión también pasa por muchos filtros que realmente hacen necesaria una responsabilidad

¹⁴ Lacruz Mantecón, M.L. “Robótica y responsabilidad civil: el daño cibernético” en Revista General de Jurisprudencia y Legislación, número 3, 2022, pp. 379-415.

objetiva. “La persona física o jurídica, autoridad, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento” de datos (“responsable” para el RGPD, art. 4 ap. 7)¹¹, actuará responsablemente si cumple con los principios y normas correspondientes. Si no lo hace, si actúa irresponsablemente, deberá asumir las consecuencias que corresponden a las usualmente conocidas responsabilidades civil, penal o administrativa. 2. El principio de responsabilidad implica, entonces, la asunción por parte del “responsable” y, en su caso, del encargado del tratamiento, de la normativa aplicable respecto a una serie de conductas que en ellos recaen como sujetos pasivos.

En ese sentido y por lo antes expuesto, incluye lo que el RGPD, art. 5.1 prevé como “principios relativos al tratamiento”: hacerlo de manera lícita, leal y transparente en relación con el interesado, recoger los datos personales con fines determinados, explícitos y legítimos y no tratarlos ulteriormente con fines incompatibles; que ellos sean “adecuados, pertinentes y limitados a lo necesario en relación con los fines (...)” (“minimización de datos”); que sean “exactos” y, en su caso, actualizarlos; limitar temporalmente el plazo de su conservación; tratarlos de manera que se garantice una seguridad adecuada, aplicando “medidas técnicas u organizativas apropiadas” (“integridad y confidencialidad”). Con este criterio, el principio de responsabilidad viene a constituir una especie de supra principio o “principio-paraguas”, que comprendería los de veracidad, finalidad, seguridad de los datos, reserva, confidencialidad, etc. Ello de alguna manera surgía de la Directiva 95/46/CE, en tanto luego de enunciar similares conductas en el art. 6.1, su apartado 2 decía: “Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1”. 3. En relación con el encargado, el RGPD, art. 28, establece el régimen aplicable. A lo previsto en el art. 17 de la Directiva 95/46/CE, nominado “Seguridad del tratamiento”, se agregan aspectos sobre la posible recurrencia a “otro encargado” (subencargado), con “autorización previa por escrito, específica o general” del responsable, y a los ítems que el contrato u otro acto jurídico que vincule a esos sujetos debe contener: objeto, duración, naturaleza y finalidad del tratamiento, tipo de datos personales, etc. y las diversas obligaciones, todas ellas dirigidas a la protección de las situaciones jurídicas en juego, en especial la de los titulares de los datos o interesados¹². Importa, también, lo que prevé el art. 26 al establecer la situación que denomina “Corresponsables del tratamiento”: “1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información (...), salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados. 2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo. 3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables”. Este último numeral protege al titular de los derechos

que integran el complejo de facultades de la protección de datos, más allá de acuerdos en que ellos no sean parte, aunque puedan acceder a su contenido. La responsabilidad aparece en calidad de “proactiva” con una configuración que lleva a que se hable del principio de accountability en tanto y en cuanto destaca el rendir cuentas (“responder, origen latino de la palabra responsabilidad) aplicada a la protección de datos personales, lo cual comprende diversos aspectos y el enfoque de que los responsables y, en su caso, los encargados del tratamiento adopten medidas de cumplimiento efectivo de la normativa¹⁵. Postula una posición preventiva y diligente y que ella pueda acreditarse en vez de un modelo reactivo, con una modalidad diversa en la operación de los datos personales. Esta nueva configuración tiene antecedente en las Directrices de la Organización para la Cooperación y el Desarrollo Económico (OCDE) de 23-IX-1980 ajustadas el 12-IX-2013 y en el Dictamen N.º 3/2010 del Grupo de Trabajo del art. 29 de la Directiva Europea 95/46/CE, de 13-VII-2010. Este expresa que los principios y obligaciones de protección de datos “no se reflejan suficientemente en medidas internas y prácticas concretas. Si la protección de datos no forma parte de los valores compartidos y las prácticas de una organización y no se asignan expresamente responsabilidades por la misma, se corre un gran peligro de que no se respeten y de que se sigan produciéndose desajustes en la protección de datos”. Al efecto propone introducir el principio de responsabilidad “que reclamaría de los responsables del tratamiento de datos la implementación de medidas apropiadas y efectivas que garantizaran” el debido cumplimiento y que lo “demostrarán cuando se lo solicitaran las autoridades de control. Ello contribuiría a que la protección de datos progresara ‘de la teoría a la práctica’ y ayudaría a las autoridades de protección de datos en sus funciones de supervisión y ejecución”. Agrega que se trata de “mostrar cómo se ejerce la responsabilidad y hacer esto verificable”¹³. En el RGPD, el “Considerando” 74 explicita tal objetivo: “Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas”^{14/ 15}.

EL INCUMPLIMIENTO Y SU RESPONSABILIDAD

En esta situación procede la aplicación de sanciones, o sea las consecuencias previstas por el ordenamiento jurídico para el caso de incumplimiento. La Directiva 95/46/CE tenía sobre este tema una previsión bajo la denominación “Responsabilidad”, art. 23, que decía “1. Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del

¹⁵ Romeo Ruiz, A. “La responsabilidad proactiva de las Administraciones públicas en la protección de datos personales” en la Revista vasca de gestión de personas y Organizaciones públicas”, número 18, 2020, pp. 138-153.

tratamiento la reparación del perjuicio sufrido. 2. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño”. A su vez, el art. 24, denominado “Sanciones”, decía: “Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva”. Esas disposiciones integraban el Capítulo III, que tenía tres artículos. 2. El RGPD tiene similares previsiones en su Capítulo VIII, pero comprende varias disposiciones, los arts. 77 a 84, cada uno de ellos con importante desarrollo, lo que condice con la aplicación directa del RGPD a los Estados y la búsqueda de uniformidad en la materia. Prevé el “derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento”, arts. 78 y 79, “sin perjuicio de los recursos administrativos o extrajudiciales disponibles”, incluido el derecho a reclamar ante una autoridad de control¹⁶. La referida tutela judicial implica varios aspectos: asegurar el acceso a la Justicia; un proceso con las garantías debidas, entre ellas para que en ese proceso las partes argumenten, aporten prueba, puedan controlar el diligenciamiento de esa u otras pruebas, que toda ella se examine y valore y, además, la certeza en lo relativo a la ejecución de la sentencia que se dicte. Relacionado con el tema, el art. 79.2 dispone que “Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad de un Estado miembro que actúe en ejercicio de sus poderes públicos”. Esta cuestión y los procedimientos de aplicación exceden el objeto de estas líneas. 3. El tema de las garantías emerge también del art. 83.8 para otro ámbito del ejercicio de la respectiva potestad, el administrativo: “El ejercicio por una autoridad de control de sus poderes en virtud del presente artículo estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y de los Estados miembros, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales” En ese sentido el “Considerando” 129 expresa: “(...) Los poderes de las autoridades de control deben ejercerse de conformidad con garantías procesales adecuadas establecidas en el Derecho de la Unión y los Estados miembros, de forma imparcial, equitativa y en un plazo razonable. En particular, toda medida debe ser adecuada, necesaria y proporcionada con vistas a garantizar el cumplimiento del presente Reglamento, teniendo en cuenta las circunstancias de cada caso concreto, respetar el derecho de todas las personas a ser oídas antes de Felipe Eduardo Rotondo que se adopte cualquier medida que las afecte negativamente y evitar costes superfluos y molestias excesivas para las personas afectadas. Los poderes de investigación en lo que se refiere al acceso a instalaciones deben ejercerse de conformidad con los requisitos específicos del Derecho procesal de los Estados miembros, como el de la autorización judicial previa. Toda medida jurídicamente vinculante de la autoridad

¹⁶ Troncoso Reigada, A; González Rivas, J.J. *Comentario al Reglamento General de la protección de datos y a la Ley Orgánica de protección de datos personales y garantía de los derechos digitales*, Pamplona: Aranzadi, 2021, vol. 2, destaca el trabajo de Villalba Cano, L. “El derecho a la tutela judicial efectiva contra el responsable o encargado del tratamiento (comentario al artículo 79 RGPD)”, pp. 3007-3018.

de control debe constar por escrito, ser clara e inequívoca, indicar la autoridad de control que dictó la medida y la fecha en que se dictó, llevar la firma del director o de un miembro de la autoridad de control autorizado por este, especificar los motivos de la medida y mencionar el derecho a la tutela judicial efectiva. Esto no debe obstar a que se impongan requisitos adicionales con arreglo al Derecho procesal de los Estados miembros. La adopción de una decisión jurídicamente vinculante implica que puede ser objeto de control judicial en el Estado miembro de la autoridad de control que adoptó la decisión”. Se indican allí, con precisión, los deberes de los órganos administrativos de control, los principios esenciales que rigen su actuación y las garantías con que deben contar las personas²⁶. 4. El art. 82, con el nomen iuris “Derecho a indemnización y responsabilidad”, trata del “derecho a recibir del responsable o el encargado del tratamiento” la indemnización por daños y perjuicios sufridos, sean materiales o inmateriales, como consecuencia de una infracción del Reglamento. El perfil de esta responsabilidad civil surge de los seis apartados de la disposición; en ella se destaca la solidaridad que emerge del apartado 4 y su motivación, ya que “Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, con arreglo a los apartados 2 y 3 responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado”²⁷. Obviamente sin perjuicio del respectivo derecho de repetición contra los demás responsables o encargados por la parte correspondiente. 5. El art. 83 establece el régimen de aplicación de multas administrativas: precisa que ellas deben poseer las condiciones propias de estas medidas, en particular ser “en cada caso individual efectivas, proporcionadas y disuasorias”. Se trata de expresiones del principio de razonabilidad propio de la juridicidad en el Derecho administrativo correctivo, enfocadas en un aspecto sustancial. El apartado 2 de este art. 83 tiene en cuenta las circunstancias que determinan la cuantía de la sanción, específicamente el elemento motivo de la sanción (“naturaleza, gravedad y duración de la infracción”, según la operación de tratamiento, el número de afectados y los daños y perjuicios; el elemento culpabilidad (“intencionalidad o negligencia”), los antecedentes del infractor, las medidas que el responsable o encargado hayan adoptado para paliar los daños, el grado de cooperación con el órgano de control, la adhesión a códigos de conducta o mecanismos de certificación, etc. El apartado 3 refiere al incumplimiento “de forma intencionada o negligente” (dolo o culpa), en relación con las operaciones de tratamiento u operaciones vinculadas, que impliquen infracción de “diversas disposiciones” del Reglamento, caso en el cual “la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves”. 6. En cuanto al régimen sancionatorio, como se dijo, procede considerar las características de la infracción. En términos de la Ley Orgánica española 3/018 de 5-XII de Protección de Datos Personales y garantía de los Derechos digitales (Preámbulo-Parte V al referir a su Título IX), el RGPD “establece un sistema de sanciones o actuaciones correctivas que permite un amplio margen de apreciación”. En ese marco, dicha ley “procede a describir las conductas típicas, estableciendo la distinción entre infracciones muy graves, graves y leves, tomando en consideración la diferenciación que el RGPD establece al fijar la cuantía de las sanciones. La categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, teniendo la descripción de las conductas típicas como único

objeto la enumeración de manera ejemplificativa de algunos de los actos sancionables que deben entenderse incluidos dentro de los tipos generales establecidos en la norma europea”. En ese sentido, entonces, la ley distingue las infracciones muy graves, graves y leves y prevé una prescripción, respectivamente, de tres, dos y un año. El instituto de la prescripción responde al valor seguridad jurídica propio del Estado de Derecho, cuando el factor tiempo no puede resultar indiferente. Asimismo, la Ley Orgánica citada, art. 75, prevé la interrupción de esa prescripción por el inicio, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente se paraliza durante más de seis meses por causas no imputables al presunto infractor. Por su parte, su art. 78 regula la prescripción de las sanciones de multa según su monto; el plazo de prescripción “comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla”. 7. De acuerdo con el RGPD las multas tienen un tope máximo de 10 millones de euros o, tratándose de una empresa, “de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía” con relación a ciertas infracciones. En otros casos, el tope máximo es de 20 millones de euros o del 4%²⁸. El art. 83.2 prevé que ellas pueden ser adicionales o sustitutivas de algunas de las medidas que adopten las autoridades de control y que establece el art. 58.2 (advertencia, apercibimiento, mandato u orden de seguir ciertas conductas (atender solicitud de ejercicio de derechos del titular de los datos, comunicar violaciones de seguridad, suspender flujos transfronterizos) y limitar o prohibir el tratamiento. De manera que la norma habilita, en algunos casos, la acumulación de más de una sanción; en cambio en otros, una de las medidas tiene un contenido que no es de esencia punitiva o aplicación de un mal jurídico como consecuencia de la infracción precedente.

Desde el punto de vista jurídico no cabe duda de la responsabilidad civil de las personas jurídicas dado que tienen capacidad de acción, y por tanto capacidad de obrar en el ámbito civil y mercantil. Pues bien, el cambio histórico es que se ha producido un Derecho Penal orientado a la persona física, pero autores como Hirsch, Tiedemann, Brender...ya plantearon hace mucho que se necesitaba un nuevo Derecho penal para las personas jurídicas¹⁷. El Derecho penal se refiere a la acción física individual o colectiva que asigna responsabilidades, por ello, muchos autores dirían, que sería más conveniente un derecho penal de la persona jurídica gradual. El problema es grave dado que el daño lo puede sufrir el gran directivo y el empleado que nada tuvo que ver en la decisión tomada. La culpa in vigilando es la que establece su propio código de disciplina y su exoneración está más o menos clara desde el punto de vista teórico. La culpa in eligendo de los ejecutores de las acciones empresariales —los empleados y directivos— es indudable que tiene que ser concretada de nuevo por nuestros tribunales. No puede ser, no es justo, que tenga la misma consecuencia jurídica decidir acciones delictivas que ejecutar las mismas con una apariencia de legalidad, como ocurre en los casos de la competencia desleal a otras empresas. Tendremos que preguntarnos dónde queda

¹⁷ Jurado Cabezas, D. “La responsabilidad penal de las personas jurídicas” en la obra colectiva *Investigaciones en Ciencias jurídicas. Desafíos actuales del Derecho*. (coord. Valencia, Ruiz, A). Málaga: Universidad de Málaga, Eumed.net, 2014, pp. 141-60.

el principio de presunción de inocencia, cuando no queda delimitada la responsabilidad. Y la negligencia como acción que genere un daño, es decir, la acción tomada sin la diligencia debida que, respetando las medidas de implementación, sin embargo, produzca daño objetivo por la sociedad o empresa. Nuestro Derecho reconoce el principio de presunción de inocencia y es la parte acusatoria quien tendrá que demostrar el daño y sobre todo la causalidad de la actuación de la empresa en ese daño. No queda resuelto este tema, y la medida de que la empresa ha implementado toda una serie de medidas anteriormente indicadas nada prueba de que realmente no se quisieran incumplir, pero también pueden fallar la vigilancia de esas medidas. Las tradicionales teorías del Derecho civil, la de la responsabilidad objetiva, la del riesgo... no parecen extrapolables a la responsabilidad penal. Una empresa o sociedad puede haber implementado un sistema de seguridad y, sin embargo, saber su punto débil para poder incumplirlo, y hablaríamos de dolo. La diligencia en la implementación de las medidas de vigilancia es un tema enormemente delicado y entendemos polémico. La comisión por omisión del deber de control es un tema dificultoso por cuanto un agente o varios pueden generar un daño que se expanda a toda la empresa. Los problemas de imputación vendrán mucho más fácilmente resueltos con una clara, diáfana y poderosa delimitación de responsabilidades de los órganos de control y vigilancia.

La primera de las leyes de la robótica, comúnmente aceptadas y acuñadas por Isaac Asimov, establece que «un robot no hará daño a un ser humano o, por inacción, permitirá que un ser humano sufra daño». Esto significa, que el principio básico de un futuro derecho de la responsabilidad de los robots deberá ser proteger al ser humano, frente a cualquier daño que pueda causarle un robot.

Y como es principio general, también del derecho, el «alterum non laedere», de cuyo incumplimiento surge la correspondiente responsabilidad civil, que generalmente se traduce en la indemnización de los daños y perjuicios causados ya de desde la *lex Aquilina*, está claro que, también en el ámbito de la robótica y de la inteligencia artificial que pueda integrarla, surgirá dicha responsabilidad por los daños y perjuicios que causen los robots y/o sus mecanismos directrices inteligentes. En el ámbito de la responsabilidad contractual el criterio de la responsabilidad objetiva o de la creación del riesgo es el que parece imponerse. Habrá que ver qué se entiende por fuerza mayor o causa excluyente de la responsabilidad (los llamados y conocidos problemas técnicos). En el campo extracontractual habría que decantarse por el riesgo creado como teoría de la responsabilidad¹⁸. Aunque también las partes son las que pueden pactar fallos o sistemas y su consecuencia en un régimen específico de responsabilidad, deberán los contratos establecer las causas técnicas más frecuentes para que ello tenga lugar. La cuestión que se plantea es la de determinar quién será el sujeto pagador de las pertinentes indemnizaciones por daños, toda vez que los robots y demás mecanismos de inteligencia automatizada, no son

¹⁸ Navas Navarro, S (y otros). *Inteligencia Artificial. Tecnología. Derecho* Valencia: Tirant lo Blanch, 2017, pp. 280 y ss.....

personas equiparables a los seres humanos y, por tanto, no pueden ser sujetos ni objeto de derechos y obligaciones personales.

Descartada la posibilidad de otorgar personalidad jurídica propia a estas sofisticadas máquinas, tan superiores a las personas humanas en muchos ámbitos, pero carentes —por el momento- de conciencia de su propio ser y de libre albedrío más allá de sus correspondientes programaciones y de su propia capacidad de aprendizaje, se han barajado al respecto varias alternativas, destacando las siguientes:

a) Trasladar la responsabilidad al fabricante del producto, asignándole la responsabilidad en caso de defectuoso funcionamiento del sistema robótico de inteligencia artificial, parece ser un criterio controlable. Teoría no aplicable por ejemplo al uso de los Drones civiles en los que el propietario responderá por el uso realizado y los daños producidos (como establece el art. 1908.1 del CC.)

b) Asignársela al usuario del robot o a aquel a quien pertenezca, como guardián de este. La primera opción, tiene la ventaja de que ya está diseñada en las leyes de responsabilidad por productos defectuosos, si bien no llega para cubrir todos los supuestos planteables, dado que el daño puede causarse por la máquina aun no siendo esta defectuosa, por un lado, y, por otro, los fabricantes del complejo integrado en el robot o sus modificaciones pueden ser muchos y difícil deslindar su responsabilidad, a costa del dañado. Debemos preguntarnos qué ocurre en el tema de la responsabilidad civil de los vehículos autónomos sin intervención del agente humano en cuanto a su conducción o funcionamiento: quizás deberíamos acudir a la responsabilidad del fabricante siempre que se hayan cumplido los estándares de revisión y otros de la maquinaria¹⁹.

La segunda opción, tiene la ventaja de que puede estar prevista en la legislación general como cláusula residual, pero su aplicación puede resultar injusta, toda vez que el usuario o poseedor del robot no es culpable de los defectos que, en origen, esté pueda presentar después de su puesta en funcionamiento automatizada y, mantener lo contrario, podría suponer la culpabilización de un inocente.

Quizás, la respuesta pase por simultanear ambos sistemas de imputación de responsabilidad, pero combinándolos con un seguro obligatorio que haga factible la integra puesta en funcionamiento automatizada y, mantener lo contrario, podría suponer la culpabilización de un inocente. Se ha planteado en el terreno jurídico en las herramientas de búsqueda y solución de litigios de forma automatizada y baremada, acerca de la responsabilidad de esos buscadores, pero en la actuación de la Abogacía esto sería un tema todavía de ciencia ficción, la e- persona y sus derechos²⁰.

¹⁹ Mugas Acosta, P. “El robot inteligente y su categorización jurídica” en la Revista Blockchain e Inteligencia Artificial, vol.3, número 4, 2022, pp.29-46.

²⁰ Martín Diz, F. “Justicia digital post covid: el desafío de las soluciones extrajudiciales electrónicas de litigios y la inteligencia artificial” en Revista de estudios jurídicos y criminológicos, número 2, 2020, pp. 41-74.

Articular disposiciones específicas, delimitando la responsabilidad por productos defectuosos de los distintos fabricantes que integren el mecanismo robótico, pero manteniendo la regla de solidaridad de todos ellos frente al dañado, incluyendo como tal al propio usuario en su caso; con la responsabilidad directa del productor y subsidiariamente del proveedor. Fijar la responsabilidad interna entre los distintos fabricantes como subjetiva y, frente al usuario, poseedor y dañado, como objetiva.

B. Ordenar el aseguramiento obligatorio de la responsabilidad por el productor, con importante cobertura y fondo de garantía en su defecto, de todas las responsabilidades derivadas del funcionamiento del robot. Establecer un derecho de repetición en caso de culpa grave de los fabricantes, para mantener un elevado estándar de calidad y contener el precio del seguro.

Y al propio tiempo, introducir en la legislación general de responsabilidad civil la llamada por «hechos de las cosas» al modo que, desde Josserand, aplica el Code francés que, precisamente, va a mantenerla tras el proyecto de reforma del año 2005, de tal forma que el usuario o poseedor, en calidad de guardián o garante del robot, deviene siempre en responsable objetivo de los daños que la máquina cause, como también puede inferirse del texto del artículo 1183 de nuestro Código civil, que tendría que enmendarse al efecto.

Tratándose de daños causados por un robot o mecanismo inteligente, de cuya utilidad se aprovecha el usuario o poseedor, pero que pueden ser causados tanto por el funcionamiento anormal, como por el normal del robot, resulta necesaria esta cláusula general de salvaguarda de responsabilidad en el derecho común, precisamente para cubrir la segunda hipótesis, en la que no entraría en juego la responsabilidad por productos defectuosos. Lógicamente, aunque el criterio de imputación residual se mantenga en el guardián o garante (usuario o poseedor), también deberá combinarse aquí el régimen de responsabilidad con el seguro obligatorio que, estando ya establecido para el fabricante, parece debiera prolongarse obligatoriamente también para aquel, a lo largo de toda la vida del robot; pudiendo estar comprendida la prima en el precio de su adquisición o arrendamiento, o abonarse por el usuario independientemente, siempre con el respaldo de un fondo subsidiario de garantía²¹.

Imaginemos el acto más personal tocante a la salud, la operación llevada a cabo por robots, por material médico autónomo, es verdad siempre dirigido por un ser humano o los supuestos de la tecnología Blockchain, entendiendo por esta esa ayuda tecnológica- incluso a distancia- compartiendo una operación quirúrgica varios médicos, dirigiéndola quien no está presente en el quirófano operante.

Si bien en el tema de la responsabilidad médica parece que las delimitaciones de responsabilidad son más claras. Aunque la ejecución puede estar robotizada y errar, la responsabilidad es del facultativo que está al frente de la intervención en este

²¹ Muñoz Villareal, A; Monterroso Casado, E. (Dir.). Inteligencia artificial y riesgos cibernéticos. Valencia Tirant lo Blanch, 2019, y en concreto el trabajo de Monterroso Casado, E. “Responsabilidad civil por daños causados por robots en el ámbito sanitario”, pp. 101-143.

sentido no variaría en nada la teoría de la responsabilidad patrimonial en el caso de la Sanidad pública.

Otro concepto problemático son los supuestos Cyborg, es decir, aquellos en que ciertas funcionalidades humanas son reconstruidas, sanadas o ayudadas por dispositivos tecnológicos especiales, supone un avance como el párkinson, la epilepsia, la traumatología, la oftalmología...tantas y tantas especiales donde esta herramienta y la nanotecnología pueden actuar y ayudar. La responsabilidad en este tema sanitario tiene que ser específica, y desde luego, no puede excluir al Estado en el funcionamiento normal o anormal de su sanidad²².

Es cierto que es un producto que al estar en el mercado queda sometido a la legislación general de los consumidores y usuarios, quedando clara la responsabilidad del fabricante, pues el enfermo, es en este caso, un claro consumidor de su tecnología especializada, pero la del Estado es clara en la autorización y control de este tipo de dispositivos... se pone en tela de juicio la teoría clásica de la responsabilidad en la que se basó siempre nuestro 1902 del Código civil. Y es que, por acción en el producto, por omisión de determinados requisitos. Se ha causado un mal a otro, y ha intervenido culpa o negligencia, algo que se ha planteado en innumerables ocasiones con el tema de las vacunas COVID y sus efectos secundarios.

Todo lo anterior puede tener cierta utilidad al momento actual. Pero, probablemente, los conceptos manejados se vean superados por la realidad de los vertiginosos avances tecnológicos en el campo de la inteligencia artificial, si se llegan a crear seres artificiales que adquieran conocimiento de su propio ser y, quizás entonces, con sus extraordinarias capacidades, dispongan y legislen ellos para nosotros. Entonces y, aunque no sea solución mágica, nace una nueva responsabilidad que transformará la teoría tradicional del daño y la responsabilidad con total seguridad.

²²Fossaceca, C.A. "Aproximaciones a la responsabilidad civil médica en la Revolución industrial 4.0" en la revista Prudentia iuris, argentina, número 90, 2020, pp.117-158.