LA GOBERNANZA DE LOS RIESGOS DIGITALES: DESAFÍOS Y AVANCES EN LA REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL*

THE GOVERNANCE OF DIGITAL RISKS: CHALLENGES AND DEVELOPMENTS IN THE REGULATION OF ARTIFICIAL INTELLIGENCE

José Vida Fernández
Profesor Titular de Derecho Administrativo
Universidad Carlos III de Madrid

Recibido:21.01.2022 / Aceptado:25.01.2022
DOI: https://doi.org/10.20318/cdt.2022.6695

Resumen: Los riesgos digitales constituyen una nueva categoría dentro de los riesgos globales que se encuentra en continuo crecimiento por lo que reclaman urgentemente su gestión y control. Estos riesgos digitales presentan una naturaleza singular por lo que tienen que ser sometidos a un modelo de gobernanza específico que actualmente se encuentra en construcción. En la configuración de este nuevo modelo de gobernanza destaca la estrategia que se está siguiendo en torno a la inteligencia artificial ya que concentra todas las claves de lo que será la futura gobernanza de los riesgos digitales en general.

Palabras clave: regulación, tecnologías de la información y la comunicación, inteligencia artificial, Derecho digital, riesgos digitales.

Abstract: Digital risks constitute a new category within global risks that are continuously growing and therefore urgently require management and control. These digital risks are unique in nature and must therefore be subject to a specific governance model that is currently under construction. In the configuration of this new model of governance, the artificial intelligence strategy stands out, as it concentrates all the keys to what will be the future of general governance of digital risks.

Keywords: information technologies regulation, artificial intelligence, digital law, digital risk.

* El presente trabajo se ha realizado como parte del proyecto de investigación "El impacto de la inteligencia artificial en los servicios públicos: Un análisis jurídico de su alcance y consecuencias en la asistencia sanitaria" (PGC2018-098243-B-I00) que se desarrolla bajo la dirección del profesor José Vida Fernández dentro de la convocatoria 2018 de «Proyectos de I+D de Generación de Conocimiento» del Programa Estatal de Generación de Conocimiento y Fortalecimiento Científico y Tecnológico del Sistema de I+D+i del Ministerio de Ciencia e Innovación.

I. Introducción: La necesaria gobernanza de los riesgos digitales

1. La imparable transformación digital que están experimentado los países desarrollados ha dado lugar a una creciente preocupación por las implicaciones negativas que conlleva este proceso. Cada vez más nuestra sociedad depende de unas tecnologías de la información y de la comunicación que están alterando todas nuestras actividades (económicas, sociales, personales) y que comprendemos y controlamos cada vez menos. El progresivo aumento de la importancia de estas tecnologías en nuestra existencia obliga a reflexionar sobre los riesgos que incorporan y que pueden suponer una amenaza a nuestras condiciones de vida.

2. Conforme a este planteamiento, los riesgos digitales están en condiciones de ser incluidos entre los propios de la "sociedad del riesgo"[1] en cuanto riesgos derivados del desarrollo tecnológico que, como el cambio climático, las epidemias o el terrorismo, amenazan nuestra existencia a nivel global. En efecto, la definición de los riesgos digitales no se limita en trabajo a las amenazas sobre la integridad de las redes y sistemas de información que afronta la ciberseguridad, sino que tienen un sentido más amplio y profundo, ya que engloba todas las transformaciones derivadas de la digitalización que pueden llegar a amenazar aspectos básicos de nuestra actual forma de vida en términos económicos, políticos o sociales.

3. En este sentido, los riesgos digitales presentan una naturaleza muy singular en tanto no comprometen físicamente nuestra supervivencia como ocurre con los riesgos medio ambientales, sanitarios o para la seguridad pública. Por el contrario, los riesgos digitales afectan a los derechos y libertades e incluso a nuestro sistema político, ya que, además de a la intimidad de las personas, implica a la libertad de expresión, las libertades políticas y al propio funcionamiento de la democracia, al principio de igualdad y, en última instancia, a la dignidad humana.

4. Las singulares características de los riesgos digitales hacen más problemático su reconocimiento y abordaje ya que requieren un tratamiento específico por parte de los poderes públicos, que no pueden limitarse a la intervención reactiva que se ha empleado hasta ahora con respecto a los avances de las tecnologías de la información y la comunicación. La creciente complejidad e intensidad de las amenazas derivadas de la digitalización hace necesaria una verdadera gobernanza de los riesgos digitales basada en medidas proactivas que garanticen una innovación tecnológica segura y respetuosa con los fundamentos de nuestro orden político, económico y social.

5. Debe tenerse en cuenta que el concepto de gobernanza se utiliza aquí en sentido amplio y flexible para dar cabida a todas las nuevas formas en que articulan las políticas públicas para hacer frente a los riesgos digitales, lo que va más allá de las tradicionales formas de intervención pública de carácter unilateral y vertical. Por lo tanto, el sentido de que se dota a la gobernanza en este sector incorpora otras muchas fórmulas además de la tradicional regulación entendida como intervención basada en normas vinculantes, y que apelan a la ética y a la iniciativa privada horizontal, como es el caso de la autorregulación (Nickel, 2015:185). En definitiva, la gobernanza es el término más expresivo y certero para denominar la nueva forma que tienen los poderes públicos de gestionar los riesgos digitales. Por último, debe aclararse que se trata de la gobernanza desarrollada a nivel europeo, ya que el análisis aquí desarrollo se circunscribe a este modelo, por lo que se dejan al margen otros que se están desarrollando en otros ámbitos como son el chino, ruso o el estadounidense, que son radicalmente distintos.

6. A partir de estas aclaraciones y con el planteamiento indicado, el presente trabajo aborda la cuestión de las gobernanza de los riesgos digitales a partir del análisis de la singularidad de dichos riesgos frente al resto de los restos globales (apartado 2), lo que constituye la base para entender la

[1] En el conocido concepto que fue inicialmente acuñado por Ulrich Beck (1998) y (2008), y que ha sido recogido a nivel interno en nuestro país en los trabajos de José Esteve Pardo tanto por lo que respecta al riesgo medio ambiental (1999) como a los riesgos para la salud (2002).

evolución que está experimentando la gobernanza del riesgo en este ámbito y el tránsito hacia un nuevo modelo (apartado 3), que se está manifestando en la estrategia que actualmente se aplica a los riesgos de una tecnología específica como es la inteligencia artificial (apartado 4).

II. La singularidad de los riesgos derivados de los entornos digitales

1. La difícil toma de conciencia de los riesgos digitales

7. Como punto de partida para plantear cualquier reflexión sobre la gobernanza de los riesgos derivados de la transformación digital resulta imprescindible tener en cuenta la singularidad que presentan esos riesgos de los entornos digitales, ya que su naturaleza y las características que presentan condicionan tanto la estrategia como los instrumentos que deben emplearse para afrontarlos.

8. En efecto, a partir de un análisis somero de los riesgos propios de los entornos digitales puede comprobarse que éstos se distinguen de los demás riesgos existentes a nivel global en la actualidad como son los riesgos medio ambientales, sanitarios, nucleares o terroristas. No es que sean más importantes, más graves o más acuciantes, sino que son, simplemente, distintos.

9. Esta singularidad se deriva, en primer lugar, de la naturaleza que presentan estos riesgos por razón del objeto que se amenaza, ya que en el caso de los "riesgos digitales" o, mejor dicho, "riesgos en entornos digitales", el objeto a proteger no es el "entorno digital" (que sería el origen del riesgo)[2] sino los derechos fundamentales, la libertad humana y, en última instancia, la dignidad de la persona que se pueden ver afectadas de muy distintas formas (vulneración de la intimidad, discriminación o exclusión social) en los entornos digitales. De este modo, cuando se habla de riesgos "para la salud" o "para el medio ambiente" el objeto a proteger (la salud, el medio ambiente) es un fin en si mismo que se manifiesta forma directa, física y concreta. Por el contrario, en el caso de los riesgos digitales nos encontramos con que el objeto a proteger (los derechos fundamentales y la dignidad humana) es abstracto y convencional y, sobre todo, se manifiesta de manera indirecta ya que lo que se tiene que proteger son esos derechos y la dignidad, y no el entorno digital que precisamente los amenaza.

10. Esta singular naturaleza de los riesgos digitales hace que sean más difíciles de identificar por parte de la ciudadanía, que es la que tiene que iniciar un debate sobre los mismos para afrontarlos a través de las medidas necesarias que se articulan a través de la llamada gobernanza. Esta inconsciencia de la ciudadanía frente los riesgos digitales es, precisamente, lo que Ulrich Beck identifica como "un reconocimiento demasiado frágil" (Beck, 2020), ya que pone en contraste la dificultad para percibir los daños sufridos en el ámbito digital con respecto a la concienciación generalizada que generan acontecimientos como el desastre de Chernóbil, el calentamiento global o la pandemia del COVID-19, en los que se produce una situación catastrófica con daños físicos concretos que genera una toma de conciencia y la adopción de medidas para afrontar estos riegos. Por el contrario, conforme aumenta la complejidad del mundo tecnológico, más disminuye nuestra comprensión del mismo y de la propia realidad que nos rodea (Bridle, 2020), de modo que los riesgos en el ámbito digital son cada vez más inciertos, más complejos y, por lo tanto, más difíciles de identificar.

11. Incluso aunque se lleguen identificar estos riesgos digitales y los daños concretos que puedan derivarse de los mismos, lo cierto es que no son percibidos como verdaderos daños. En este sentido debe recordarse que, en el ámbito digital ha habido desastres que han desvelado daños muy graves a escala mundial, como el sistema de Vigilancia Prism de la NSA revelado por Edward Snowden o el de Cambridge Analytica con Facebook[3], y, sin embargo, estos sucesos no han provocado una conciencia-

[2] Esto siempre que se entiendan los riesgos digitales en un sentido amplio, más allá de la ciberseguridad, ya que, de lo contrario, el objeto amenazado sí sería el entorno digital, esto es, la seguridad de las redes y sistemas de información.

[3] Sobre el sistema de vigilancia (Prism) de la Agencia de Seguridad Nacional desvelado por Edward Snowden se puede

ción y movilización ciudadana similar a la que existe en defensa del medio ambiente o de la salud. Por el contrario, estos escándalos se han disuelto con el tiempo sin que hayan puesto en guardia a la ciudadanía, que desconoce y subestima el verdadero alcance de los daños causados, aunque resulte evidente que el número de personas afectadas y las consecuencias de la vulneración masiva de la intimidad de las personas o de su manipulación han tenido consecuencias fatales. El problema es que, en el fondo, los daños que se sufren en los entornos digitales no son considerados verdaderos daños ya que la violación de nuestra libertad y pérdidas de los derechos no duele, sino que desaparecen sin que los seres humanos resulten físicamente dañados (Beck, 2020: 313).

12. Pero, aún más, aunque esos riesgos digitales y los daños que puedan derivarse de los mismos sean considerados como verdaderos riesgos, lo cierto este que, en gran medida, se trata de riesgos y daños que son consentidos, lo que dificulta la movilización ciudadana. En efecto, existe una fuerte tendencia dataísta en nuestras sociedades ya que se asume como algo natural la renuncia a determinados derechos y libertades para alcanzar un estadio superior en la evolución (Harari, 2016) a través del poder de los datos y de su procesamiento masivo mediante sistema digitales. Sin necesidad de entrar en el debate al respecto, es posible constatar que la mayoría de los ciudadanos se deslizan por esta pendiente del dataismo, ya que asumen los riesgos e, incluso, soportan estoicamente los daños que puedan derivarse del uso de determinados servicios digitales como un precio necesario para disfrutar de las soluciones y funcionalidades que dichos servicios les ofrecen[4].

2. La creciente amenaza de los riesgos digitales y la urgencia de su gobernanza

13. Todas estas circunstancias, junto al más tardío desarrollo de la revolución tecnológica en este ámbito, han provocado que, a diferencia de lo que ocurre con otros riesgos globales, no hayamos sido conscientes de la gravedad y trascendencia que pueden llegar a tener los riesgos digitales hasta tiempos muy recientes, a pesar de la creciente amenaza que representan.

14. En efecto, los riesgos en el ámbito digital no se limitan a la vulneración de nuestra intimidad, sino que puede alcanzar a nuestra propia esencia que es el libre albedrío, limitando o haciendo desaparecer nuestra propia condición humana. Así puede apreciarse en numerosos estudios que alertan sobre la capacidad de las tecnologías digitales para captar nuestra atención (Wu, 2020), para atraparnos en un determinado marco ideológico o "filtro burbuja" y condicionar nuestros pensamientos y opiniones (Pariser, 2020) o someternos de manera voluntaria a un poder que nos conoce mejor que nosotros mismos (Han, 2014). E incluso, más allá de este condicionamiento indirecto de nuestra voluntad, se están desarrollando tecnologías mucho más directas e invasivas que permiten registrar datos mentales a partir de los impulsos cerebrales y manipular dichos datos reintroduciendo nuevos impulsos, que han motivado el reconocimiento tanto en Chile como en España de los neuroderechos para preservar la integridad física y psíquica del individuo[5].

15. Además, la evolución, alcance y consecuencias de estos riesgos digitales son muy distintos a los de los demás riesgos globales, no ya por su singular naturaleza, sino porque se producen en un escena-

consultar el libro del propio Snowden (2020) y, en el caso de Cambridge Analytica, y su incidencia en las elecciones presidenciales de los EEUU de 2017 que concluyeron con la victoria de Donald Trump resulta recomendable la lectura de Kaiser (2020)

[4] Así puede comprobarse en el caso de Google Maps que rastrea de forma permanente a sus usuarios para ofrecerles las mejores rutas, o, en el caso de los asistentes inteligentes (como Alexa, Siri o OK Google) a los que se permite que monitoricen las conversaciones a cambio de poder utilizar todas sus funcionalidades.

[5] Chile está desarrollando los trámites necesarios para ser el primer país que reconozca los neuroderechos en su Constitución a través de la modificación de su artículo 19, número 1°, para proteger la integridad y la indemnidad mental con relación al avance de la inteligencia artificial. Al respecto *vid*. Bastidas Cid (2021)

En el caso de España, el reconocimiento tiene un alcance mucho más limitado, ya que la Carta de Derecho Digitales, aprobada por Acuerdo del Consejo de Ministros de 13 de julio de 2021 dedica su apartado XXVI a las neurotecnologías estableciendo que pueden regularse por Ley los límites y garantías de implantación y empleo en las personas de las neurotecnologías.

rio inédito hasta ahora, ya que la innovación tecnológica no se centra en el control y explotación de la naturaleza, como ocurre con los demás riesgos. Por el contrario, estamos en la "era del capitalismo vigilante" (Zuboff, 2020) en la que se controla y explota a los humanos por parte de unas grandes corporaciones que, por razones tecnológica, económicas y jurisdiccionales, escapan del alcance de los poderes públicos. Se está generando, por primera vez, un imperio regido por grandes empresas en el que puede llegar a ejercerse unos niveles de control desconocidos hasta ahora en la medida en que las personas nos estamos volviendo transparentes (Beck, 2020: 313). Frente a este nuevo escenario los derechos fundamentales tradicionales son insuficientes ya que fueron concebidos, en su mayoría, como derechos para limitar y contener el poder del Estado (es el caso de la interceptación de comunicaciones o, en general, las libertades políticas -censura, manifestación, etc.-) y, por el contrario, a lo que nos enfrentamos es a un poder absoluto de unos sujetos privados frente al que sólo podemos luchar, por ahora, invocando la protección de nuestra intimidad.

16. Por último, debe repararse en lo imparable del proceso de digitalización al que estamos sometidos, cuya intensificación en estos últimos años incrementa exponencialmente el nivel de los riesgos que este conlleva. Se trata de un proceso irreversible que va a ir en aumento en tanto todos los Estados, empresas y demás sujetos privados hacen depender su crecimiento y desarrollo de la digitalización. En el caso de la Unión Europea, la Comisión Europea afirma que estamos viviendo lo que identifica como "la década digital" y ha planteado una entrega incondicionada a lo digital, como puede apreciarse en sus planes para los próximos años que se contienen en la Comunicación Brújula Digital para 2030 de marzo de 2021[6] y en la financiación del Programa Europa Digital 2021-2027[7] y el Mecanismo de Recuperación y Resiliencia[8]. Pero lo más dramático es que la digitalización, que aquí se analiza como el origen del riesgo, se ha convertido en la panacea absoluta y definitiva, incluso para superar los demás riesgos globales como los sanitarios (las aplicaciones para controlar la pandemia provocada por la COVID), los ambientales (el fomento de los medios digitales para reducir la contaminación) o para la seguridad (los sistemas de vigilancia para controlar el terrorismo internacional)[9]. De este modo se genera una perversa correlación inversa conforme a la que la reducción del nivel de los riesgos globales más graves (para el medio ambiente, la salud o seguridad) pasa por el incremento de los riesgos en el ámbito digital.

17. Todas estas circunstancias hacen que sea urgente la incorporación de una verdadera gobernanza que gestione y mitigue estos riesgos digitales que van incrementándose y agravándose, y que no pueden afrontarse con las medidas adoptadas hasta ahora. De este modo, y a pesar de las dificultades descritas que han retrasado el debate sobre las amenazas derivadas de la transformación digital, en los últimos años ya se han estado adoptando algunas medidas que adelantan un cambio de paradigma en la identificación y tratamiento de los riesgos digitales configurando así un nuevo modelo de gobernanza de los riesgos digitales

III. Evolución y características de la gobernanza de los riesgos digitales

1. El punto de partida desde una intervención de mínimos

18. La singular naturaleza de los riesgos digitales explica las diferencias existentes entre el modelo de gobernanza que se emplea en este ámbito y los que se aplican para afrontar los demás riesgos

[6] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Brújula Digital 2030: el enfoque de Europa para el Decenio Digital, COM (2021) 118 final, 9 de marzo de 2021.

[7] Reglamento (UE) 2021/694 del Parlamento Europeo y del Consejo, de 29 de abril de 2021, por el que se establece el Programa Europa Digital y por el que se deroga la Decisión (UE) 2015/2240 (DOE 11.5.2021 L 166/1).

[8] Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021 por el que se establece el Mecanismo de Recuperación y Resiliencia (DOE 18.2.2021 L 57/17).

[9] Incluso a nivel teórico algún autor como Thomas Hemphill (2020:7) recomienda como principal instrumento para la gobernanza de la innovación (y del riesgo en general) el "adoptar la inteligencia artificial y el análisis de datos para la gestión de riesgos y el ajuste de la regulación", sin reparar que los riesgos que, a su vez, entraña ese remedio.

globales. Como puede comprobarse sin gran dificultad, en el caso de los riesgos sanitarios, medio ambientales o para la seguridad, la gobernanza se ha basado en una intervención extraordinaria tanto por el número de medidas adoptadas como por su variedad y, sobre todo, por su intensidad. Así, por ejemplo, las actividades relacionadas con los medicamentos (salud) o con los organismos modificados genéticamente (medio ambiente) se encuentran sometidos a un régimen de intervención administrativa que se proyecta con una fuerza extraordinaria en todo su ciclo e implica, entre otras, medidas como la exigencia de autorización para la investigación, desarrollo, puesta en el mercado, etc.; y en el caso de la seguridad, la medidas son igualmente contundentes ya que implican medidas de vigilancia y prohibiciones, aunque no lleguen a conocerse la totalidad de las medidas adoptadas.

19. Por el contrario, la intervención que se ha desplegado hasta ahora para afrontar los riesgos en el ámbito digital se ha basado en unas medidas de carácter mínimo, ya que han sido pocas, indirectas y de alcance muy limitado. De hecho, puede afirmarse que, desde sus orígenes, los avances que se han venido produciendo en las TICs han estado sometidas únicamente a unas medidas basadas en límites externos establecidos tanto por normas generales (como son las normas sobre seguridad de productos y servicios y de protección de los consumidores) como por normas específicas (como la normativa sobre servicios de sociedad de la información –o servicios digitales– y, sobre todo, por la normativa de protección de datos personales). Esto al margen de la existencia de una normativa de estandarización (o normalización) destinada a mejorar la seguridad y calidad de productos y servicios que es de cumplimiento voluntario.

20. A pesar de la aparente densidad de toda esta normativa, la innovación digital se ha desplegado tradicionalmente bajo un principio de libertad, sin que haya sido obstaculizado el desarrollo y puesta en el mercado de los avances, ya que se han venido aplicando medidas de carácter negativo, *ex post* y estrictamente reactivas-correctivas, que, por lo tanto, han funcionado como límites externos. El ejemplo más expresivo de esta intervención de mínimos está en la evolución de Internet, la innovación que más han transformado nuestra sociedad en las últimas décadas, y que se ha desarrollado sin que exista una única Ley que lo regule de forma específica, ya que se han ido desplegando distintas normas destinadas a proteger aspectos que podían verse afectados por esta innovación (intimidad, propiedad intelectual, derechos de los consumidores), estableciéndose así unos límites externos que han encauzado su desarrollo.

2. El cambio de paradigma hacia una nueva gobernanza de los riesgos digitales

21. Si bien el desarrollo de las TICs se había basado en ese principio de libertad concretado en una intervención mínima, desde comienzos de la década pasada se puede apreciar un cambio de modelo motivado por la creciente importancia de la transformación digital para el crecimiento económico y el desarrollo social, y la necesidad de que exista un entorno de confianza y seguridad para que dicha transformación se produzca. La relevancia estratégica de lo digital está llevando a que muchos países vayan abandonando su tradicional modelo de intervención negativa y de carácter pasivo para desplegar una nueva estrategia de gobernanza de los riesgos en el ámbito digital que implica una mayor intervención.

22. Así se puede apreciar con especial claridad en el caso de la Unión Europea que, como es conocido, se ha venido caracterizando tradicionalmente por el despliegue de una importante intervención pública sobre las actividades económicas. No obstante, se trata de una tendencia generalizada que se proyecta a nivel global ya que se replica igualmente en otros ordenamientos como el estadounidense o los latinoamericanos con distintos planteamientos y diferente intensidad.

23. El punto de partida de este cambio de paradigma se sitúa en una nueva generación de normas de protección de datos que, en el caso de la Unión Europea se contienen en el Reglamento General de

Protección de Datos[10] de 2016 y que se han ido incorporando igualmente a diferentes países, y que se caracterizan por incorporar medidas positivas, *ex ante* y esencialmente proactivas-preventivas, con las que se implica a los particulares de forma activa en el cumplimiento de normativa adaptando el cumplimiento a cada caso, en línea con los principios de la innovación responsable.

24. Estas medidas se concretan, en primer lugar, en el principio de responsabilidad proactiva, por el cual, el responsable del tratamiento no solo debe cumplir con la normativa de protección de datos, sino que deberá ser capaz de demostrarlo[11]. A este principio se suma al enfoque orientado a la gestión del riesgo que obliga a la evaluación del riesgo para determinar las medidas de seguridad dependiendo del nivel de riesgo existente[12]. Y ambos principios se unen en la obligación de la protección de datos desde el diseño y por defecto que exige aplicar medidas apropiadas para la protección de datos, atendiendo al estado de la técnica, coste y naturaleza del tratamiento y el riesgo que conlleva para los derechos y libertades de los afectados[13]. A esto se suman otras medidas complementarias que contribuyen a la responsabilidad activa como la figura del delegado de protección de datos y los mecanismos de autorregulación a través de códigos de conducta y de co-regulación mediante las certificaciones[14].

25. Como puede comprobarse la normativa de protección de datos se sitúa a la vanguardia de este nuevo modelo de gobernanza del riesgo en el ámbito digital y establece un canon que se proyecta en todo este ámbito. Por lo tanto, el cambio que se ha producido en la protección de datos no tiene carácter aislado, sino que ha venido acompañado de otros muchos cambios que se han venido introduciendo, tanto en la normativa sectorial específica aplicable a TICs (servicios digitales online, inteligencia artificial, etc.), como también en la normativa general que le resulta de aplicación como es el caso de las normas sobre seguridad de productos y servicios, sobre protección de los consumidores, etc.

26. Se trata, por tanto, de un cambio de paradigma que se extiende a toda la transformación digital y que pone de manifiesto el progresivo abandono del tradicional *laissez faire* que se había practicado ante los avances tecnológicos que se venían dando en el ámbito de las TICs, y que tiene su origen en la creciente preocupación por los riesgos que pueden entrañar determinadas innovaciones tecnológicas con un enorme potencial disruptivo como es el caso de las plataformas de servicios digitales o la inteligencia artificial.

27. Por lo que respecta a las grandes plataformas, se puede apreciar claramente este cambio de paradigma en las nuevas iniciativas que ha puesto en marcha la Unión Europea con la propuesta de sendas Leyes de servicios y de mercados digitales que introducen una verdadera regulación *ex ante* de estas actividades que hasta ahora se habían desarrollado con total libertad bajo un régimen jurídico de mínimos como servicios de la sociedad de la información[15]. El caso de la inteligencia artificial presenta

[10] Se trata del conocido Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (DOU 4.5.2016 L 119/1).

[11] El artículo 5 del RGPD establece que «*el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1* (que se refiere los principios relativos al tratamiento de los datos) *y capaz de demostrarlo («responsabilidad proactiva»)*».

[12] Conforme al artículo 35 RGPD.

[13] Así se prevé que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas tendiendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento y se añade que debe aplicar dichas medidas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento (art. 25 RGPD).

[14] Sección 4 y 5 respectivamente del Capítulo IV RGPD.

[15] Se trata de las Propuestas de Reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales) y sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales), presentadas el 15.12.2020 COM(2020) 825 final, que vienen acompañadas por otras medidas ya en vigor como la Directiva (UE) 2019/770 sobre contratación de contenidos y servicios digitales y el Reglamento (UE) 2019/1150 servicios de intermediación en línea para usuarios profesionales, que conforman lo que se puede identificar como el nuevo régimen de los servicios digitales Vida Fernández (2021).

mayores novedades ya que se trata de una tecnología inédita sobre la que se proyectan todas las novedades de la nueva gobernanza, por lo merece un análisis más detallado que se desarrolla más adelante.

3. Características de la nueva gobernanza de los riesgos digitales

28. Aunque el nuevo modelo de gobernanza de los riesgos digitales se encuentra en proceso de formación y tendrá que definirse en los próximos años, ya es posible constatar que no es equiparable a los modelos de gobernanza de los demás riesgos globales. En efecto, la naturaleza singular de estos riesgos digitales que se ha descrito anteriormente, hace que sea muy difícil desplegar un sistema de intervención similar al que se ha venido desarrollando frente a los riesgos que amenazan el medio ambiente, la salud o la seguridad, por lo que deberá desarrollar unas características propias que aún están por definir.

29. Sin embargo, la construcción de la gobernanza de los riesgos digitales no puede plantearse en términos adánicos al margen de los demás modelos de gestión de los riesgos globales. Por el contrario, una gran parte de sus principios, instituciones y estructura están siendo asumidos en la gestión de estos nuevos riesgos derivados de la transformación digital. Así puede comprobarse en el caso del principio de precaución que está presente en la gobernanza de los riesgos digitales y que goza de una especial relevancia, tal y como puede comprobarse en la propuesta de reglamento de ley de inteligencia artificial de la Unión Europea que, sin mencionarlo, contiene importantes medidas de intervención ex ante –como prohibiciones y obligaciones–. Por lo tanto, no puede afirmarse que en el ámbito digital el principio de precaución haya sido superado por el principio de innovación, otro principio que ha ido surgiendo en los últimos tiempos aunque, por ahora, carece de reconocimiento formal en el Derecho europeo o nacional, ya que su mención se limita a documentos informales que lo describen como un "impulso a aquella regulación que favorezca la innovación manteniendo los estándares de protección de los derechos y valores reconocidos por la Unión"[16]. En todo caso, precaución e innovación no son principios contrapuestos sino complementarios ya que se trata de evitar interpretaciones maximalistas que puedan frenar o desbocar el desarrollo tecnológico y generar medidas que sean flexibles y se adapten a cada caso para afrontar los riesgos.

30. Ahora bien, en la configuración del modelo de gobernanza de los riesgos digitales, se irán forjando nuevos principios, instituciones y mecanismos que tienen su sentido y proyección en este ámbito específicos, como es el caso de las evaluaciones de riesgos que surgieron en el ámbito de la protección de datos y que se van aplicando a otras dimensiones de las innovaciones tecnológicas que van surgiendo en el ámbito digital bajo la denominación de evaluaciones de impacto. En efecto, este tipo de evaluaciones están ahora extendiéndose y desarrollándose en otros ámbitos de la digitalización como son los sistemas de inteligencia artificial, en los que adquieren nuevas funcionalidades ya que no se limitan a tener en consideración únicamente cuestiones relacionadas con la privacidad sino que se obliga a tener en consideración otros aspectos como la discriminación o la exclusión, lo que implica incorporar estándares socio-técnicos para valorar estos riesgos lo que, sin duda, va a complicar enormemente la evaluación.

31. Por lo que se refiere a la estrategia a través de la que se va a desarrollar este nueva gobernanza de los riesgos digitales, parece muy difícil que se despliegue a través de una intervención ordenada y sistemática con unos instrumentos únicos y homogéneos y, menos aún, se prevé ningún tipo de código con principios y mecanismos comunes que se apliquen de forma más o menos general, tal y como suele ocurrir en el ámbito del medio ambiente o de la salud. Por el contrario, parece inevitable que se produzca una intervención fragmentada ya que es necesario mantener un tratamiento diferenciado de las diversas aplicaciones y servicios que se enmarcan dentro del ámbito digital y de sus distintas dimensiones (protección de datos, propiedad intelectual e industrial) en tanto responden a diferentes principios

[16] European Political Strategy Centre (EPSC), «Towards an Innovation Principle Endorsed by Better Regulation», EPSC Strategic Notes nº 14, 30 de junio de 2014.

y valores, y presentan su propia problemática. Así, por ejemplo, no puede aplicarse un mismo régimen de responsabilidad por sus servicios a los prestadores de servicios de sociedad de la información (como por ejemplo una página de venta de productos online) que a los que prestan servicios electrónicos de confianza (como es la firma electrónica cualificada) o los que los que prestan servicios de inteligencia artificial, ya que tiene que ser necesariamente asimétricos para ajustarse a los distintos principios, valores y problemáticas que concurren cada caso.

32. De este modo, no es posible identificar unas técnicas únicas para abordar los riesgos en entornos digitales, ya que estas dependerán de las características de los problemas que se plantean en cada caso. En efecto, en la gestión de los riesgos digitales se han venido desarrollando una gran cantidad de técnicas de carácter muy variado y complejo –*horizon scanning, scenario planning, upstream public engagement, constructive technology assessment, real-time technology assessment, ethical technology assessment, sandboxes*, códigos de conducta, estándares, moratorias, etc. (Stilgoea, Owen, Macnaghten: 2013)–, pero todas ellas vienen aplicándose de forma abierta y flexible sin que prevalezca ni se excluya ninguna de ellas, de modo que utilizan desde las más rudimentarias como la prohibición de actividades), a las más sofisticadas como la experimentación en s*andboxes* o bancos de prueba.

33. Más allá de este esbozo de trazo grueso, poco más se puede concretar del nuevo modelo de gobernanza de los riesgos derivados de los entornos digitales ya que, como se ha adelantado, se encuentra en pleno proceso de desarrollo sin que hayan terminado de concretarse las que serán sus principales características.

IV. La gobernanza de los riesgos digitales en el ámbito de la inteligencia artificial

1. Del soft law a las propuestas de regulación de la inteligencia artificial

34. Si bien, como se ha indicado, el cambio de paradigma en la gestión de los riesgos derivados en los entornos digitales tiene su origen en la normativa de protección de datos, el proceso de transformación se está extendiendo por todas las dimensiones del sector digital, adquiriendo un especial significado en el ámbito de la inteligencia artificial que constituye el ejemplo más novedoso y completo de este cambio. En efecto, el desarrollo durante los últimos años de sistemas cada vez más complejos y eficaces de inteligencia artificial y la expectativa de que se apliquen a cada vez más ámbitos de la actividad humana ha generado una creciente preocupación a nivel global que se está concretando en numerosas medidas en las que se ponen de manifiesto las características del nuevo modelo de gobernanza de los riesgos digitales.

35. En el caso de la Unión Europea, la preocupación en torno a los desafíos que plantea la inteligencia artificial ha motivado un intenso debate que se ha desarrollado tanto a nivel europeo como nacional donde se han aprobado distintas estrategias por parte de los países europeos[17]. En el caso de la Unión Europea resulta muy destacable que, en poco más de tres años, se haya fraguado una verdadera política específica en esta materia que ha culminado con la presentación de una propuesta de Reglamento sobre inteligencia artificial.

36. Así, a partir de las Conclusiones Europeo de 19 de octubre de 2017 [EUCO 14/17], en las que se apuntaba a la necesidad de abordar los riesgos de la inteligencia artificial, la Comisión publicó la Comunicación Inteligencia Artificial para Europa el 25 de abril de 2018 COM(2018) 237 final, a la

[17] En el caso de España se aprobó una Estrategia Nacional de Inteligencia Artificial el 20 de noviembre de 2020. Otros países europeos han aprobado su propia estrategia como es el caso de Francia (*Donner du sens à l'intelligence artificielle: pour une stratégie nationale et européenne*, de 8 de marzo de 2018), Alemania (*Strategie Künstliche Intelligenz der Bundesregierung*, de 15 de noviembre de 2018) o del Reino Unido (*AI in the UK: No Room for Complacency*, de 15 de diciembre de 2020).

acompañaría el Libro Blanco sobre Inteligencia artificial de 19 de febrero de 2020 COM(2020) 65 final. En paralelo, el Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial publicó unas Directrices Éticas en materia de IA el 8 de abril de 2019 y el Parlamento Europeo aprobó el 20 de octubre de 2020 tres importantes documentos: una resolución con recomendaciones a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial 2020/2012(INL); un informe sobre responsabilidad por daños derivados de la inteligencia artificial 2020/2014(INL); y un informe sobre los derechos de propiedad intelectual y el desarrollo de la inteligencia artificial 2020/2015(INI). Toda esta evolución ha concluido (por ahora) con la propuesta de Reglamento sobre normas armonizadas sobre inteligencia artificial presentada por la Comisión Europea el 21 de abril de 2021.

37. Lo más relevante de todo este proceso es que la Unión Europea ha articulado una sólida política en materia de inteligencia artificial, con medidas de intervención sólidas y contundentes con las que se ha superado la indeterminación y el carácter dispositivo que sufría está política basada en inicialmente en medidas de *soft law*. De esto modo, la estrategia europea sobre inteligencia artificial se ha articulado en tres instrumentos complementarios a través de los que se lleva a cabo la gobernanza de los riesgos derivados de este avance tecnológico: las directrices éticas, los procesos de estandarización y el marco jurídico general y específico[18].

38. En primer lugar, las directrices éticas del Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial de abril de 2019 constituye un instrumento de *soft law* que contiene un enfoque ético de la inteligencia artificial centrada en el ser humano y basada en directrices como la predictibilidad, explicabilidad, responsabilidad y respeto de los derechos fundamentales, que trata de convertirse en un punto de referencia a nivel internacional al hacer de la Unión Europea el adalid de la IA ética y fiable, dando lugar así a un modelo propio y distinguible en el materia (AI made in Europe).

39. Aunque carezcan de carácter vinculante, las directrices éticas tienen un importante papel ya que son la manifestación de la horizontalidad, flexibilidad y adaptabilidad del nuevo modelo de gobernanza. En todo caso, la falta de vinculatoriedad no resta de valor jurídico a las directrices éticas que cumplen numerosas funciones. Así, constituyen un punto de referencia para los Estados que pueden utilizarlas como fundamento tanto para la estandarización como para la configuración de las normas que les puedan resultar aplicable en tanto ofrecen criterios para abordar los riesgos que vayan apareciendo con la intensificación del uso de la inteligencia artificial. La utilidad de este marco ético es indudable ya que contiene principios generales que constituyen un punto de encuentro y que actúan como faro que guía el proceso de incorporación de la inteligencia artificial. Sin embargo, sus virtudes son también el origen de sus problemas ya que la falta de concreción y vinculatoriedad impide que se puedan encontrar soluciones únicas dando lugar a una fragmentación que ha hecho necesaria la adopción un marco normativo armonizador.

40. En segundo lugar, estaría la estandarización o normalización que es un instrumento de autorregulación regulada que sirve para que el diseño, desarrollo o utilización las soluciones de IA cumplan unos parámetros comunes dispuestos por los propios actores del sector bajo la supervisión pública. Se trata así, de unos mecanismos de co-regulación que sirven para la normalización de los productos conforme a unas "normas" y "reglamentos técnicos" (como los de la ISO) cuya observancia se acredita mediante actos de certificación de entidades privadas acreditadas o de homologación por la Administración pública. Aunque esas normas y reglamentos técnicos no tienen carácter vinculante, generan efectos jurídicos en tanto la presunción de conformidad con las mismas facilita la libre circulación y la aceptación por el mercado, resultando un mecanismo idóneo para el control de la inteligencia artificial[19].

[18] Tal y como los sistematiza Hernández Peña (2020) que desarrolla un análisis detallado de cada uno.

[19] Tal y como apunta Galán Pascual (2021:13) y como propone Vega Iracelay (2018: 39) como modelo de una adecuada gobernanza.

41. Sin duda la normalización va a jugar el papel más relevante en la gobernanza de la inteligencia artificial ya que se trata de un instrumento idóneo que incorpora elementos como el carácter técnico de detalle, la adaptabilidad, la flexibilidad, que son necesarios para encauzar una tecnología compleja y de vanguardia como es la inteligencia artificial. En este sentido se puede comprobar como la IA ha pasado a figurar de forma permanente en los Planes de Regulación de Estandarización para TIC (*Rolling Plan for ICT Standardisation*) aprobados por la Unión Europea, como es el caso del último de 2021 que la identifica como uno de los ámbitos estratégicos y habilitadores en los que se desarrollará la política europea de estandarización, para lo que plantea incorporar actores relevantes (empresas, administraciones, universidades, sociedad civil), coordinarse con los procesos desarrollados a nivel internacional, y considerar las directrices éticas del Grupo de Expertos. En la actualidad se están desarrollando los primeros estándares o normas técnicas en esta materia por parte del Comité Europeo de Normalización (CEN) y los representantes nacionales que permitirán incorporar la ética y la seguridad desde el diseño, sin necesidad de recurrir a imposiciones.

42. En tercer y último lugar, el marco jurídico o la regulación a través de normas de *hard law*, se presenta como un instrumento residual dentro de la gobernanza de la inteligencia artificial, ya que se aplica ante las insuficiencias de los anteriores. En efecto, aunque las normas y reglas son el instrumento de intervención más clásico y natural, se plantean como recurso de *ultima ratio* dentro de la gobernanza en este ámbito en el que priman otros instrumentos que tratan de implicar a los actores y evitar la imperatividad para garantizar el cumplimiento y acierto de unas exigencias en un contexto que es extremadamente complejo.

43. No obstante, el incremento de los riesgos derivados del uso de sistemas de inteligencia artificial ha otorgado un mayor protagonismo al marco jurídico al que debe quedar sometida esta tecnología, que se está completando y reforzando con la propuesta de normas específicas que van a regular estos sistemas, tal y como se podrá comprobar a continuación.

2. Análisis del marco jurídico de la inteligencia artificial

44. Como punto de partida a la hora de analizar el marco jurídico de la inteligencia artificial es necesario aclarar que, pese a lo que pudiera parecer, esta novedosa tecnología ya se encuentra regulada, si bien no está sometida a un régimen jurídico específico. En efecto, en todos los ordenamientos es posible encontrar un buen número de normas que, de forma fragmentada e indirecta, resultan aplicables a esta nueva tecnología y a los avances que va experimentando.

45. En efecto, en el ámbito de la Unión Europea los sistemas de inteligencia artificial quedan sometidos a numerosos bloques normativos, que pueden ordenarse de la siguiente manera conforme a un criterio de especificidad concluyendo con los más generales. En primer lugar, y en tanto se basan en el procesamiento masivo de datos estos sistemas se someten a la normativa de protección de datos (RGPD), a la de circulación de datos no personales (Reglamento de Datos no Personales)[20] y la de datos abiertos y reutilización de información del sector público (Directiva Open Data[21]). En la medida que pueda considerarse un servicio de las TICs se le aplica la normativa sobre sociedad de la información (Directiva de Comercio Electrónico[22]) y la normativa sobre servicios digitales que vendrá a sustituirla (las futuras directivas de servicios y mercados digitales[23]). También en el ámbito de la normativa digi-

[20] Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

[21] Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público.

[22] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.

[23] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley

tal, y en tanto le resulte aplicable por sus características se aplicaría la normativa sobre ciberseguridad (como la Directiva NIS[24] o el Reglamento sobre Ciberseguridad[25]).

46. Por otra parte, como cualquier otro producto o servicio se le aplica la normativa general sobre seguridad y responsabilidad de productos incluidas en el *New Legislative Framework*[26] de 2008 y el futuro Reglamento de seguridad de los productos[27] y la Directiva de máquinas[28]. En la medida que estos sistemas estén destinados o afecten a consumidores finales se aplicará la normativa general sobre consumidores y usuarios[29]. Y en cuanto estos sistemas de inteligencia artificial se empleen en ámbitos económicos concretos sometidos a una regulación específica se le aplicará el contenido de la normativa de referencia laboral, de salud, de transporte, etc. Todo esto sin perjuicio de que deben respetar el contenido de los derechos fundamentales reconocidos tanto la Carta de Derecho Fundamentales de la UE como en el Convenio Europeo de Derecho Humanos.

47. A pesar de la aparente densidad de toda esta normativa, debe tenerse en cuenta que se trata de un marco jurídico de mínimos que es indirecto e inespecífico, por lo que aplica a todas las innovaciones que van surgiendo en el ámbito digital. De esta forma, cualquier programa de software que se desarrolle –incluso aunque no esté basado en inteligencia artificial–, quedaría sometido a la misma normativa que actúa básicamente, como un límite externo a las innovaciones.

48. Precisamente por ello, toda esta normativa se ha venido completando a nivel europeo con medidas de *soft law* basadas en el establecimiento de principios de conducta (directrices éticas) y de autorregulación regulada (normalización). Sin embargo, todas estas medidas han sido consideradas insuficientes para afrontar los riesgos que plantean los sistemas de inteligencia artificial, por lo que la Comisión Europea ha recurrido a normas jurídica (*hard law*) directas y específicas como es la Propuesta de Reglamento del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de inteligencia artificial) COM(2021) 206 final que fue presentada el 21 de abril de 2021 y que se adoptará a lo largo de 2022. Se trata de una iniciativa que pone de manifiesto el cambio de paradigma en la gobernanza de los riesgos digitales ya que se abandona el abstencionismo que tradicionalmente había caracterizado a las políticas en el ámbito digital y se recurre a una intervención a través de medidas *ex ante* de carácter proactivo para afrontar los eventuales riesgos derivados de la inteligencia artificial.

---

de servicios digitales) COM(2020) 825 final y Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales) COM/2020/842 final.

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

[25] Reglamento 2019/881 del Parlamento europeo y del Consejo relativo a ENISA (Agencia europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento 526/2013 (Reglamento sobre la Ciberseguridad).

[26] Que se compone del Reglamento (CE) Nº 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos; la Decisión Nª 768/2008/CE del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre un marco común para la comercialización de los productos; y el Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos

[27] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la seguridad general de los productos, por el que se modifica el Reglamento (UE) n.º 1025/2012 y se deroga la Directiva 87/357/CEE y la Directiva 2001/95/CE

[28] Se trata de la modificación de la Directiva 2006/42/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a las máquinas

[29] Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011 , sobre los derechos de los consumidores, a la que se añade la Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior y también la Directiva 2006/114/CE del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006 , sobre publicidad engañosa y publicidad comparativa

49. En todo caso, debe tenerse en cuenta que esta propuesta de Reglamento de Ley de inteligencia artificial no establece un marco jurídico completo y exhaustivo en este ámbito, sino que viene a completar la normativa que ya resulta aplicable para cubrir las cuestiones más problemáticas que pueden surgir de determinados usos de la inteligencia artificial. Además, esta propuesta de Reglamento no supone el desembarco de las medidas tradicionales de intervención pública (prohibiciones, licencias, autorizaciones) como las que se han desarrollado frente a los riesgos medioambientales, sanitarios o de seguridad, sino que incorpora una serie de disposiciones que, si bien son de carácter vinculante, tienen un carácter abierto, flexible y adaptativo al igual que las que se venían aplicando en el ámbito de la protección de datos.

50. Sin entrar en un análisis detallado de la propuesta de Reglamento, lo más destacable desde el punto de vista estratégico es la unidad y contundencia con la que la Unión Europea ha decidido reforzar la gobernanza de esta materia, ya que se opta por un reglamento como instrumento de intervención normativa, para evitar así cualquier posible fragmentación entre los Estados miembros a la hora de establecer unas reglas específicas para los principales problemas que suscita la inteligencia artificial[30]. En todo caso, se trata de un reglamento peculiar ya que no contiene un régimen acabado de la inteligencia artificial, sino que establece unos contenidos mínimos que admiten ser completados por los Estados Miembros[31].

51. Por otra parte, el futuro Reglamento sobre inteligencia artificial tiene un carácter transversal y expansivo ya que tendrá un alcance extraterritorial al aplicarse a usuarios y prestadores situados en terceros Estados cuando el resultado producido por el sistema se utilice en la Unión, lo cual resulta esencial para la eficacia de su contenido en la medida que gran parte de las actividades pueden ser desarrolladas por prestadores fuera de la UE[32]. En este mismo sentido, la propuesta de Reglamento se proyecta al uso de la IA, tanto en el ámbito privado como público, teniendo en cuenta las particularidades que presenta su utilización por las autoridades públicas[33].

52. La finalidad de esta propuesta de Reglamento no es otra que afrontar y gestionar los riesgos que suscita el uso de la inteligencia artificial, y es precisamente el concepto de "riesgo" el que se convierte en el eje de su diseño[34]. En la configuración de la gestión de los riesgos de esta nueva tecnología se ponen de manifiesto las principales características de la nueva gobernanza de los riesgos digitales ya que establece un marco jurídico específico para la inteligencia artificial, en el que se incorporan distintas técnicas de intervención, con un enfoque abierto, proporcionado y flexible como corresponde a la nueva gobernanza de los riesgos en este ámbito.

53. Conforme a estas características, lo más notable de la propuesta es que se basa en un enfoque orientado a riesgos, que da lugar a una intervención adaptativa que se ajusta al nivel de riesgo generado por los distintos usos de la inteligencia artificial que se clasifican en[35]:

a) Riesgo inadmisible, que se enumeran de forma taxativa (por ejemplo, cuando se trata de sistemas que manipulan colectivos vulnerables, o la identificación biométrica en tiempo real en espacio públicos) y que quedan expresamente prohibidos[36];
b) Riesgo alto, que es el concepto clave ya que son sistemas que se enumeran en un Anexo

[30] Apartado 2.4 de la exposición de motivos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de inteligencia artificial) COM(2021) 206 final.

[31] Sobre el reglamento como instrumento para la ordenación de la inteligencia artificial *vid.* García García (2022: 319)

[32] El artículo 2 de la Propuesta de Reglamento dispone que será aplicable a: a) Quienes introduzcan o pongan en servicio sistema de IA en el territorio de la Unión Europea, al margen de que estos proveedores tengan establecimiento en la UE o en terceros países; b) Quienes utilicen sistemas de IA que se encuentren dentro de la UE; c) Cualquiera de los anteriores que estén situados en terceros países, cuando la infracción de salida generada sea usada dentro de la UE.

[33] Por ejemplo, la naturaleza de los algoritmos (Boix Palop, 2020) o el acceso a los mismos (Gutiérrez David, 2021).

[34] Hasta el punto de que se hace mención a los riesgos más de trescientas veces a lo largo del Reglamento.

[35] Para un análisis más detallado del sistema de riesgos contenido en la propuesta de Reglamento de Ley de inteligencia artificial *vid*. Soriano Arnanz (2021: 11-20).

[36] Título II (artículo 5) sobre Prácticas de Inteligencia Artificial Prohibidas.

que se irá modificando y que dependen del ámbito en que se utilicen. Estos sistemas están permitidos, pero deben cumplir ciertos requisitos y someterse a un control ex ante de cumplimiento de los mismos, donde se apreciar el enfoque orientado a riesgos en tanto se facilita y flexibiliza su utilización siempre que evidencien la seguridad de los mismos a través de la de la autocertificación y la estandarización[37];

c) Riesgo limitado, que incluyen sistemas que se relacionen con humanos, o que manipulan contenidos (como es el caso del *deep fake*) a los que se impone unas obligaciones de transparencia, esencialmente para que se identifique su presencia[38];
d) Riesgo mínimo o nulo, que son aquellos sistemas de inteligencia artificial que se aplican de forma muy específica y en tareas sin especial trascendencia (filtros de spam, videojuegos), cuyo uso es libre, aunque se fomenta el cumplimiento de códigos de conducta para adecuarse a los requisitos del riesgo alto.

54. Por otra parte, la propuesta de reglamento incorpora técnicas de gobernanza novedosas, como puede comprobarse en las medidas para el fomento de la innovación[39], entre las que se encuentra la creación de bancos de prueba regulatorios (*sandboxes*) para un uso controlado de nuevas soluciones de inteligencia artificial.

55. Por último, resulta notable la propuesta de una estructura organizativa específica para la gestión de esta nueva gobernanza de los riesgos derivados de la inteligencia artificial[40], ya que se prevé que los Estados miembros designen una autoridad nacional de supervisión que será la responsable de la ejecución del reglamento de forma objetiva e imparcial, y , asimismo, se dispone la creación de una Comité Europeo de Inteligencia Artificial como organismo de cooperación y consulta que servirá a las autoridades nacionales de supervisión.

56. En definitiva, de aprobarse en estos términos, la propuesta de la Reglamento supondrá un importante avance, ya que es un compendio de los mejores y más avanzados instrumentos para la gobernanza de los riesgos en el ámbito digital, por lo que resulta imprescindible tenerla como punto de referencia.

V. Conclusiones

57. Los riesgos digitales constituyen una realidad frente a la que es necesario actuar, a pesar de las dificultades que han existido hasta ahora para su identificación y toma de conciencia por parte de la ciudadanía. El imparable proceso de transformación digital está incrementando el alcance y la trascendencia de estos riesgos que se han convertido en una creciente amenaza, por lo que se hace necesaria e inaplazable la reacción por parte de los poderes públicos.

58. Sin embargo, los riesgos digitales presentan una naturaleza propia y singular que los distingue de los demás riesgos globales, por lo que requieren de un sistema de gobernanza específico. En este sentido, se trata de unos riesgos que no afectan a una realidad física ni amenazan nuestra existencia material, sino que se proyectan sobre todas nuestras actividades afectando a nuestro sistema económico y político, así como a nuestros derechos y libertades y, en última instancia, a nuestra dignidad como personas.

59. La novedad que suponen estos riesgos y la falta de una verdadera concienciación frente a los mismos explican la ausencia, hasta ahora, de un sistema de intervención pública para la gestión de los avances en el ámbito digital. A pesar de la enorme trascendencia que la informatización de la sociedad o

[37] Título III (artículos 6 a 51) sobre sistemas de inteligencia artificial de alto riesgo.
[38] Título IV (artículo 52) sobre Obligaciones de transparencia para determinados sistemas de inteligencia artificial.
[39] Título V (artículos 53 a 55) sobre Medidas de Apoyo a la Innovación.
[40] Título VI (artículos 56 a 59) sobre Gobernanza.

el acceso permanente a infinidad de datos, los avances tecnológicos que lo han permitido, como son los ordenadores personales, la programación informática o Internet, se han desarrollado bajo un marco de plena libertad sometidos a unas medidas de carácter mínimo meramente reactivas y de carácter negativo.

60. La intensificación de la transformación digital y la creciente relevancia de los riesgos que conlleva este proceso están provocando un cambio de paradigma que se manifiesta en el surgimiento de una nueva gobernanza de los riesgos digitales a nivel europeo con la que se abandona el tradicional abstencionismo frente a la innovación tecnológica que se había venido practicando en el ámbito de la TICs.

61. Esta nueva gobernanza europea de los riesgos digitales tiene su primera manifestación en el ámbito de los datos, en el que la Unión ha adoptado una serie de iniciativas encabezada por el Reglamento General de Protección de Datos que incorpora medidas de carácter positivo que implican actuación proactiva tanto por parte de los particulares bajo la supervisión de los poderes públicos.

62. La construcción de esta gobernanza a nivel europeo se proyecta ahora sobre la inteligencia artificial, cuyo desarrollo ha suscitado una gran preocupación y ha precipitado la adopción de numerosas iniciativas de manera que se puede empezar a hablar de un incipiente sistema de gobernanza de los riesgos digitales y a identificar sus elementos característicos.

63. En concreto la política europea sobre inteligencia artificial se materializa en distintas medidas tanto de carácter dispositivo (*soft law*) como vinculantes (normas), que implican la actuación de los actores privados concernidos como de las autoridades públicas competentes y que se combinan entre ellas de forma flexible y abierta. Así pueden sistematizarse todas estas medidas en tres niveles como son los principios (directrices éticas), la auto y co-regulación (estandarización) y la regulación ordinaria (normativa).

64. Incluso esta última modalidad de gobernanza a través de medidas de intervención normativa, incorpora importantes novedades ya que no se basa en instrumentos de intervención unilateral, cerrada y estática (autorizaciones, licencias) sino que incorpora un enfoque abierto y adaptativo basado en la valoración del riesgo por parte de los particulares, junto a otras novedades que van forjando el nuevo sistema de gobernanza de los riesgos digitales.