INTELIGENCIA ARTIFICIAL Y DERECHOS DE PARTICIPACIÓN POLÍTICA

Artificial intelligence and political participation rights

JOSÉ ANTONIO MONTILLA MARTOS[1]

RESUMEN: En este trabajo se analizan los riesgos derivados de Inteligencia Artificial para los derechos de participación política de la ciudadanía, por la posible incidencia en los procesos electorales. A partir de ello, se apuntan las líneas de actuación más adecuadas para abordar esos riesgos. En ese sentido, se destaca la importancia que puede tener el futuro Reglamento europeo de Inteligencia Artificial si finalmente es aprobado con los elementos que permitan el control, evaluación y sanción de los sistemas e instrumentos de Inteligencia Artificial que puedan afectar a los procesos electorales, al condicionar de forma subliminal la actuación de los electores.

PALABRAS CLAVE: Inteligencia artificial, derechos fundamentales, derechos de participación política, procesos electorales.

ABSTRACT: This paper analyzes the risks derived from Artificial Intelligence for the rights of political participation of citizens, due to the possible incidence in electoral processes. Based on this, the most appropriate lines of action are pointed out to address these risks. In this sense, the importance that the future European Artificial Intelligence Regulation may have if it is finally approved with the elements that allow the control, evaluation and sanction of the Artificial Intelligence systems and instruments that may affect electoral processes, by subliminally condition the actions of voters.

KEYWORDS: Artificial intelligence, fundamental rights, rights of political participation, electoral processes.

[1] Catedrático de Derecho Constitucional. Universidad de Granada. E-mail: montilla@ugr.es

I. INTRODUCCIÓN. INTELIGENCIA ARTIFICIAL Y DERECHOS

Los beneficios de la Inteligencia Artificial (IA) para el progreso social son evidentes. Están presentes en cualquier ámbito de la vida, desde la medicina a los servicios sociales, la seguridad, la movilidad, la lucha contra el cambio climático, la eficiencia de los sistemas de producción, etc. Pero, lógicamente, también se advierten los riesgos de una tecnología que, en definitiva, plantea sustituir la actuación de las personas por las máquinas a través de programas informáticos en el desempeño de determinadas tareas, a fin de mejorar la eficiencia. Hay quien considera a la IA como una amenaza para la supervivencia de la especie humana. Sin llegar a esas posiciones apocalípticas nos enfrentamos a un fenómeno disruptivo que está provocando una transformación de la economía y la sociedad.

Los juristas tenemos una función específica en este contexto. A las ciencias cognitivas (filosofía, ética, fisiología, neurociencia, lingüística) le corresponde establecer el marco teórico; a las ingenierías, el funcionamiento técnico; y a los juristas la integración de la IA en la vida social planteando una regulación que, tras evaluar sus riesgos para la vida en sociedad y el contrato social que la rige, el ordenamiento constitucional, proponga respuestas desde ese ordenamiento para intentar conjurarlos. En este sentido, no se trata simplemente de abordar las novedades conflictuales que la IA provoca en el tráfico jurídico sino de dar respuesta a su incidencia en los pilares esenciales de la organización política de la sociedad como los derechos fundamentales o la democracia pluralista.

Ciertamente, a medida que esa tecnología ha ido avanzando, ha crecido en paralelo una preocupación institucional por sus posibles consecuencias, en especial por su afectación a los derechos y libertades de la ciudadanía y, en general, al funcionamiento democrático de nuestras sociedades en el marco de un Estado constitucional. Por ello, en los últimos años están apareciendo numerosos documentos, especialmente en el ámbito de la UE y del Consejo de Europa, aportando reflexiones sobre la forma de abordar esta cuestión. Una reflexión que, a medida que avanza la aplicación efectiva de la IA, se va trasladando del ámbito de la ética al Derecho y, específicamente, al Derecho Constitucional.

El reto al que se enfrenta el Derecho en general, y el Derecho Constitucional en particular, no es fácil. Las constituciones se han elaborado para un mundo analógico y el mundo digital ha cambiado su objeto (J.F. Sánchez Barrilao, 2016, 239). Los factores de poder que actúan en el mundo digital no se ajustan a las previsiones constitucionales. En este sentido, la Constitución, como conjunto de normas que regulan la organización política de la sociedad para la limitación del poder, tiene una posición difícil en el nuevo orden digital. No obstante, continúa siendo necesario en este contexto limitar y controlar la actuación del poder. Un poder que ya no es sólo público sino que, de forma novedosa, lo ejercen actores privados como son las grandes compañías tecnológicas sobre las que gira el desarrollo de la IA y tienen, en consecuencia, una gran capacidad potencial de influencia en el espacio público. Es lo que el profesor Balaguer ha denominado “constitucionalizar el algoritmo” en el sentido de aplicar los límites derivados de los principios y valores constitucionales a una realidad digital que tiene, obviamente, una dimensión constitucional (F. Balaguer Callejón, 2022: 30, 181-191).

En concreto, la dimensión constitucional del algoritmo debe abordarse en relación a los derechos (F. Balaguer Callejón, 2022: 40-49). Hemos de atender a la relación entre el uso de herramientas o sistemas basados en la IA y los derechos fundamentales. Es evidente el riesgo de que los derechos fundamentales sean masivamente vulnerados a través de la IA o incluso que se conviertan en accesorios de los derechos vinculados al mercado. Además, como hemos indicado, esa afectación no procede ya de los poderes públicos sino de actores privados que actúan en ese ámbito público. En el Informe elaborado por la Agencia de Derechos Fundamentales de la Unión Europea (FRA), denominado "Construir correctamente el futuro. La inteligencia artificial y los derechos fundamentales" (2021) se explica que la atención de la IA se ha centrado hasta ahora en su potencial para contribuir al crecimiento económico. Sin embargo, el modo en que las diferentes tecnologías pueden afectar a los derechos fundamentales había suscitado un menor interés pese a resultar constatada la posible vulneración de diversos derechos. Ya el Libro Blanco sobre Inteligencia Artificial, publicado por la Comisión Europea el 19 de febrero de 2020, en el que se resumen los principios más destacados de un futuro marco normativo de la UE para la IA, hacía hincapié en la protección de los derechos. Y es que, en efecto, el futuro de la IA pasa por establecer un marco jurídico, a partir de principios éticos, en el que se garanticen los derechos fundamentales recogidos en las distintas declaraciones de derechos, todas ellas con un contenido similar, sea en textos internacionales, en las constituciones nacionales o en la Carta de Derechos Fundamentales de la Unión Europea. La regulación jurídica no va a evitar los riesgos que conlleva la revolución tecnológica para los derechos fundamentales pero el establecimiento de límites coadyuva a su salvaguardia.

Cuando se concretan los derechos especialmente en riesgo por la irrupción de la IA, los documentos institucionales, especialmente de la Unión Europea, como el mencionado informe de la Agencia de Derechos Fundamentales (FRA) se refieren al derecho a la privacidad, a la protección de datos, a la no discriminación o al acceso a la justicia. La obtención y uso masivo de datos es el presupuesto para la aplicación de la IA por lo que el derecho a la protección de datos de carácter personal se convierte en una suerte de derecho de referencia y al usar los datos suelen generarse discriminaciones algorítmicas o sesgos en perjuicio de colectivos históricamente preteridos que vulneran el derecho a no ser discriminado. A partir de esos presupuestos, se ha advertido preocupación por otros derechos: intimidad, secreto de las comunicaciones, acceso a la justicia, etc.

Se ha prestado hasta el momento menor atención a los derechos de participación política. Sin embargo, esa incidencia existe y, además, resulta especialmente trascendente. La interferencia de las grandes compañías tecnológicas en el derecho a la protección de datos personales o en el derecho a no ser discriminado puede ser instrumental para la afectación de los derechos de participación política, en concreto el derecho a un sufragio libre, igual, directo y secreto. La gestión masiva de datos de forma automatizada, controlada por algoritmos, conlleva su uso para configurar perfiles que no sólo pueden ser de consumidores sino también de electores. De esta forma, la IA interfiere en el ejercicio de los derechos de participación política como se ha demostrado en los casos de las elecciones presidenciales norteamericanas de 2016 o en el referéndum del Brexit de ese mismo año.

En el proceso de obtención y gestión de datos se pueden vulnerar diversos derechos fundamentales pero al usar esos datos para interferir en el proceso político no sólo se están vulnerando derechos fundamentales de las personas sino que se está poniendo en cuestión el propio funcionamiento del proceso electoral, clave de bóveda de una democracia pluralista. No estamos ante la mera búsqueda de un beneficio económico con vulneración de derechos de la personalidad, lo que ya es especialmente grave. Ocurre que al afectar al derecho de participación política se está condicionando el propio proceso democrático, la elección de nuestros representantes y, por tanto, la esencia de la democracia pluralista. Esa es la cuestión a la que me quiero acercar de forma tentativa en las siguientes páginas.

II. LA INTELIGENCIA ARTIFICIAL PERMITE AVANCES EN EL FUNCIONAMIENTO DEMOCRÁTICO DE LA SOCIEDAD PERO TIENE IMPORTANTES RIESGOS

La utilización de la IA ha permitido mejoras en el funcionamiento democrático de la sociedad. En sus primeros años de expansión, Internet y las redes sociales fueron recibidos como una suerte de ágora, que permitía nuevas formas de participación y, en definitiva, posibilitaba avanzar de una democracia representativa a una democracia más participativa. Como nos decía Bobbio, se abría la posibilidad de retornar a la libertad de los antiguos, en la dicotomía de Constant, mediante la ampliación de los espacios de democracia directa gracias a la tecnología (N. Bobbio, 2003: 413). Supuso, en efecto, la aparición de un nuevo espacio público virtual que permitió novedosas formas de participación. Una de las primeras experiencias en ese sentido fue el proceso de elaboración del Tratado por el que se establece una Constitución para Europa. En los trabajos de aquella Convención, creada rememorando la Convención de Filadelfia, pudo participar la ciudadanía europea a través de la plataforma creada al efecto. Desde entonces, comprobamos como los mecanismos de participación y también de reivindicación de la ciudadanía han resultado facilitados en el marco de la sociedad digital.

La democracia de Internet y las redes sociales es, obviamente, más participativa. Las tecnologías de la información y la comunicación han permitido una mayor participación en las primarias de partidos políticos o en la celebración de consultas de distinto tipo. Incluso, se han impulsado experiencias de voto electrónico, aunque ha planteado un debate específico en el que no podemos detenernos. En cualquier caso, hay ventajas de la digitalización para los procesos electorales que, a mi juicio, resultan claras.

Es evidente, por otro lado, que el ejercicio del derecho de acceso a la información pública puede resultar favorecido por el desarrollo de la sociedad digital en general y de la IA en particular, en cuanto permite gestionar cantidades masivas de datos. Y esto no sólo a través de los cauces formalizados, como puede ocurrir en España con el portal de transparencia en el marco de la Ley 19/2003, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, sino también a través de cauces menos formalizados pues cualquier persona, física o jurídica, puede compartir a través de sistemas de IA una ingente cantidad de información pública, lo que enriquece el debate y favorece la constitución de una opinión pública libre e informada.

Sin embargo, esa imagen idealizada de Internet y las redes sociales para la evolución hacia una democracia más participativa y, en definitiva, para la expansión de la democracia en el mundo se ha visto cuestionada al advertirse distintos elementos que distorsionan el adecuado funcionamiento del sistema democrático. Internet permite una mayor libertad en el flujo de información y comunicación. Por ello, los regímenes autoritarios tienden a bloquearlo. Sin embargo, esos efectos benéficos para la democracia resultan contradichos al menos por dos fenómenos ínsitos a su propia naturaleza. Por un lado, la gestión privada de estos procesos; por otro, que su propia lógica de funcionamiento favorece la polarización de la sociedad y, con ello, refuerza las posiciones políticas populistas y extremistas, dañando el propio funcionamiento de la democracia pluralista.

La primera distorsión deriva, por tanto, de que buena parte de estos procesos no son gestionados desde lo público con la finalidad de mejorar el funcionamiento de la sociedad sino intermediados por compañías globales de carácter privado cuyo único interés es el beneficio económico. Los datos personales aportados en un proceso participativo o de acceso a información pública son acumulados y reelaborados con el fin de utilizarlos como mercancía. En este sentido, la idea de que las redes sociales y las nuevas formas de comunicación habilitaban una participación más libre se ha cuestionado al comprobar que permite una utilización mercantil con la intención de incidir en el comportamiento de las personas no sólo como consumidores sino también, en lo que ahora nos interesa, como electores. No es posible la participación directa, sin mediadores, en cuanto las grandes compañías tecnológicas se han convertido en mediadores necesarios que controlan los procesos comunicativos (F. Balaguer, 2022: 73-80). De esta forma, estos actores privados de carácter global son sujetos de poder en condiciones de vulnerar los derechos y libertades de la ciudadanía y, en concreto, los derechos de participación política.

Por otro lado, a estas alturas de desarrollo digital, está plenamente asumido que la sociedad digital y, en concreto, las redes sociales favorecen la polarización de la sociedad, al menos por dos motivos.

En un primer sentido, ofrecen un trato preferente a las posiciones más extremas frente a las más moderadas, sin que siquiera sea esa su intención o coincida con su ideología. Simplemente, se constata que los mensajes más radicales y escandalosos son los que más visitas tienen en cualquier plataforma digital, incluso por pura curiosidad. Por ello, los algoritmos que rigen el tratamiento automatizado de los mensajes en esas plataformas dan prioridad a estos mensajes pues están diseñados para lograr el mayor beneficio económico y mientras más visitas reciban, más publicidad estarán en condiciones de contratar y, con ello, mayor beneficio económico. No se incorpora la responsabilidad social. Incluso, da igual que los mensajes sean verdaderos o falsos pues el algoritmo no discrimina ni valora desde una perspectiva ética. De esta forma, estamos ante un auténtico círculo vicioso. Como los mensajes radicales tienen más eco y, con ello, generan más beneficios se anteponen a otros más moderados aunque ello conlleve una mayor polarización de la sociedad y el crecimiento de posiciones políticas extremistas.

Además, por otro lado, las compañías tecnológicas elaboran a través de los algoritmos un perfil psicológico de cada uno de los usuarios a partir de sus búsquedas para trasladarles los mensajes que más les puedan interesar, atendiendo a su forma de pensar. De esta forma, se constituyen grupos cerrados y autorreferenciales que consolidan sus principios. La relación de los usuarios suele reducirse a aquellos que piensan de forma similar lo que, en su envés, dificulta el diálogo con los que piensan diferente. Con ello, no se está ayudando a construir un espacio público común en el que se puedan alcanzar acuerdos y grandes consensos sociales sino que, por el contrario, lo dificulta. Ya lo explicaba Tony Judt en *Algo va mal*: "formaremos comunidades globales de afinidades electivas pero perderemos el contacto con las afinidades de nuestros vecinos" (T. Judt, 2010: 120).

III. LOS RIESGOS PARA EL EJERCICIO DEL DERECHO DE PARTICIPACIÓN POLITICA DERIVADOS DE LA INTELIGENCIA ARTIFICIAL

Los graves riesgos de las tecnologías de la información y la comunicación, y específicamente de la IA, para el ejercicio de los derechos políticos se pusieron de manifiesto al denunciarse la influencia de la IA, con la intermediación de actores privados, en el referéndum del Brexit y en las elecciones presidenciales americanas de 2016. No son casos únicos pero si especialmente relevantes por la denuncia pública de la forma en que se produjeron y el escándalo que ello generó. Desde entonces se han seguido denunciando diversos intentos de desestabilizar gobiernos o influir en procesos electorales a través de la IA en distintos lugares del mundo (O. Sánchez Muñoz, 2020: 34-40). En este sentido, el riesgo de influir en el ejercicio de los derechos de participación, en los derechos del elector y del elegible, han quedado claros.

Cambridge Analytica era una empresa de gestión de datos para su utilización en procesos electorales que trabajó tanto en la campaña presidencial de Trump como en la de los partidarios del Brexit. El escándalo surgió en 2018 cuando un antiguo empleado de la compañía denunció que se usaban los datos para influir en el comportamiento electoral del votante. En el caso de las elecciones presidenciales americanas, el procedimiento era el siguiente. A través de una empresa intermediaria de estudios de mercado se ofreció una pequeña contribución a usuarios a cambio de realizar un test de personalidad, presentado como parte de un estudio científico. De esa forma, se consiguieron los datos de 200.000 personas y un consentimiento muy amplio para su tratamiento, que alcanzaba a la red de contactos. Esto permitió a la compañía estudiar los datos de muchos millones de personas, a través de una aplicación de Facebook. Con ello, a través de los datos psicográficos obtenidos se generaron sus perfiles como potenciales votantes. Una vez realizado el perfilado se hizo la intervención mediante la microsegmentación de mensajes personalizados, atendiendo a sus rasgos de personalidad, especialmente a través de Facebook. De esta forma, se intentaba canalizar su actuación política e influir en su comportamiento electoral (J. Castellanos Claramunt, 2019, 12; J.C. Hernández Peña, 2022: 47-51).

Lo que se hizo desde esta empresa, con la colaboración necesaria de Facebook, fue utilizar los patrones de conducta de proximidad o rechazo para intentar condicionar, intencionadamente y de forma subrepticia, el ejercicio de los derechos de participación

política. La customización de las redes sociales para ofrecer la respuesta que más se aproxima a las preferencias de cada persona permite también acotar, obviamente, sus preferencias políticas. Con esto ya se estaría vulnerando el derecho de participación activa pues el voto es libre, igual, directo y secreto, y nadie puede conocer nuestra opción electoral sin un consentimiento expreso. Pero ese comportamiento electoral no sólo ha sido conocido sin consentimiento sino también manipulado pues no se trataba de predecir el comportamiento electoral, como pretenden las encuestas electorales, sino de inducirlo. A partir de ese conocimiento, se han utilizado los perfiles psicológicos para remitir mensajes personalizados con la intención de orientar el comportamiento electoral. En concreto, se trataba de generar rechazo a una opción concreta para que se vote a la opuesta o el elector se abstenga.

Estamos ante una acción deliberada, no casual o involuntaria. Era un uso intencionado de datos personales que no debían ser utilizados por las plataformas al servicio de concretos intereses políticos, para modificar el comportamiento electoral. Y todo ello no de forma expresa sino subliminal. La vulneración del derecho fundamental al ejercicio del sufragio activo de forma libre, igual, directa y secreto resulta nítida.

Aunque no resulte fácil, debe distinguirse esta actuación de otras más normalizadas en los procesos electorales pero que también tienen sus riesgos. El uso de las redes sociales ha alterado completamente las campañas electorales a través de técnicas cada vez más sofisticadas. Las distintas opciones políticas siempre han querido conocer los intereses y preferencias de sus potenciales votantes, a fin de elaborar los mensajes a utilizar en las compañas electorales. Sin duda, las tecnologías de la información y comunicación han supuesto una auténtica revolución en este proceso en cuanto permiten la microsegmentación, esto es, la posibilidad de dirigir mensajes diseñados a medida a partir de los datos recopilados sobre cada persona (O. Sánchez Muñoz, 2020, 51). La propia LOREG se ha referido a esta posibilidad, como comentamos a continuación, pero parecen evidentes los riesgos al menos en dos sentidos. Por un lado, respecto a la obtención de los datos, en cuanto pueden ser obtenidos sin el consentimiento expreso del usuario o con una finalidad distinta para luego ser utilizados en campañas electores y, por otro, en relación al mensaje microsegmentado que se remite pues no es lo mismo una petición expresa de voto que el envío de mensajes con noticias falsas con las que se pretende manipular el comportamiento electoral de forma subliminal. En este segundo ámbito aparecen los riesgos específicos de la IA pues permite saber no sólo como piensa sino, sobre todo, como siente cada persona y, a partir de ahí, se puede intentar condicionar el ejercicio de sus derechos de participación política a través de mensajes aparentemente ajenos a la contienda electoral pero que provoquen aceptación o, sobre todo, rechazo (O. Sánchez Muñoz, 2020, 91; escéptico sobre los efectos de estos procesos, J.C. Hernández Peña, 2022: 59).

La influencia de estos métodos nada tiene que ver con la de los medios tradicionales, que también quieren influir en el comportamiento electoral a través de sus mensajes, de sus editoriales o incluso de las encuestas que publican.

Es cierto que la línea de separación entre conocer las preferencias e influir en dichas preferencias es tenue, y suele traspasarse con facilidad. Pero lo que debe impedirse son la campañas de manipulación digital, que con un diseño profesional y estratégico

pretenden condicionar el comportamiento del elector de forma subliminal, a través de mensajes dirigidos individualmente a él y elaborados a partir de los datos previamente obtenidos sobre sus filias y sus fobias. Esta incidencia es mayor cuando esos mensajes se transmiten de forma privada, por ejemplo a través de WhatsApp.

Cuando ese condicionamiento subliminal se hace de forma masiva, sobre millones de electores, se está desestabilizando el proceso electoral y con ello los pilares de un sistema democrático pluralista basado en la libre elección.

IV. LAS LINEAS DE ACTUACIÓN PARA AFRONTAR LOS RIESGOS PARA EL DERECHO DE PARTICIPACION POLÍTICA Y EL SISTEMA DEMOCRÁTICO PLURALISTA

El elemento positivo del asunto Cambridge Analytica es que ha supuesto una alerta global sobre los riesgos de la IA para los procesos electorales, para la democracia pluralista, y la necesidad de adoptar medidas a fin de que no se produzcan situaciones como la descrita. Se deben buscar respuestas sobre cómo aprovechar las ventajas de la IA para una mejor participación política a la vez que se conjuran los riesgos advertidos. En este momento, solo es posible hacer acercamientos tentativos en relación a cómo actuar frente a esos riesgos. A mi juicio, dicha actuación puede ir en las siguientes líneas.

1. No basta con modificar la legislación electoral

En primer lugar, para limitar la incidencia de la IA en los procesos electorales no basta con las medidas que afecten a la regulación de dichos procesos electorales. La legislación electoral no se ha adaptado a la sociedad digital. Tampoco lo ha hecho la administración electoral a fin de dotarse de herramientas para actuar en este nuevo contexto. Sin duda, habría que abordar una reforma profunda de una legislación electoral que apenas menciona la realidad digital en la que se desarrolla en la práctica y soslaya fenómenos como la desinformación en este proceso a través de mensajes manipulados, difundidos de forma masiva y microsegmentados. Debe reforzarse la transparencia en este nuevo contexto, limitando determinadas técnicas publicitarias, y la exigencia de responsabilidad a todos los intervinientes (O. Muñoz Sánchez, 2020: 230). Sin embargo, esto es necesario pero no suficiente.

En la LOREG apenas encontramos una mención a los medios digitales en relación a la prohibición de publicidad fuera del periodo de campaña electoral (art. 53). Sin duda, lo más novedoso, y polémico, en este ámbito fue la inclusión a través de la LO 3/2018, de Protección de Datos Personales y Garantía de Derechos Digitales, de un nuevo artículo 58 bis en virtud del cual los partidos políticos podían recopilar datos personales relativos a las opiniones políticas de las personas en el marco de sus actividades electorales. Esa actuación, continuaba diciendo el precepto, “se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas”. Era evidente el riesgo que esa previsión legislativa suponía en relación a la posible elaboración de perfiles a partir de opiniones políticas y la remisión de información personalizada para influir de forma subliminal en el comportamiento electoral. De hecho, inmediatamente después de su entrada en vigor, la Agencia Española de Protección de Datos elaboró un Informe en el

que rechazaba que ese precepto permitiera el "tratamiento" de los datos recopilados y sostenía su interpretación restrictiva. En cualquier caso, la STC 76/2019 ha declarado la inconstitucionalidad de esta previsión en cuanto la ley orgánica "no ha fijado por sí misma, como le impone el art. 53.1 CE, las garantías adecuadas por lo que respecta específicamente a la recopilación de datos personales relativos a las opiniones políticas por parte de los partidos políticos en el marco de sus actividades electorales. Ello constituye una injerencia en el derecho fundamental a la protección de datos personales de gravedad similar a la que causaría una intromisión directa en su contenido nuclear" (FJ 7).

Más allá de lo discutible de la medida adoptada por el legislador, nos interesa destacar esa apelación del Tribunal Constitucional a que el legislador debe concretar las garantías del uso de datos personales en el proceso electoral. Debe recordarse que la justificación del precepto declarado inconstitucional era que, en la práctica, los partidos políticos ya empleaban esos datos y se trataba, por tanto, de regular tal uso para evitar problemas y adaptarse al Reglamento UE 2016/679, del Parlamento Europeo y del Consejo, de protección de datos de las personas físicas (RGPD), al que luego nos referimos, en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. El Tribunal Constitucional apela, en definitiva, a que se adapte todo el proceso electoral al marco digital, en el que cada vez se desarrolla con mayor intensidad. Sin embargo, simplemente con esos cambios normativos no vamos a impedir que la IA se pueda utilizar para incidir en los procesos electorales; hay que intervenir también sobre la regulación de la propia IA a fin de que pueda supervisarse y garantizarse su aplicación.

2. La autorregulación no es suficiente

En segundo lugar, sostenemos que la autorregulación no es suficiente. En los últimos años las compañías tecnológicas han avanzado en la autorregulación para evitar las injerencias en los procesos políticos. Twitter ha prohibido los anuncios de carácter electoral y ha limitado la microsegmentación en los mensajes de contenido político. Google también ha excluido la orientación política como criterio de segmentación. Facebook dice haber adaptado los algoritmos para que los sitios sospechosos tengan menos presencia en la sección de noticias de los usuarios (O. Sánchez Muñoz, 2020: 104-123).

Sin embargo, no basta con la autorregulación. Es verdad que la actuación de las compañías tecnológicas está resultando relevante en la detección y eliminación de cuentas falsas en las redes sociales. Sin embargo, estas compañías se rigen por criterios de beneficio económico y, en ese sentido, su responsabilidad social está siempre condicionada por su cuenta de resultados. Por ello, los decálogos o códigos éticos no vinculantes son importantes. Debe mencionarse, en ese sentido, el Código de conducta sobre desinformación impulsado por la Comisión Europea y suscrito por Facebook, Google, Twitter, Mozilla y Microsoft. Sin embargo, debe hacerse compatible con la iniciativa reguladora de los poderes públicos.

En los orígenes de internet, los usuarios lo reivindicaban como un espacio independiente de los poderes públicos y, en ese sentido, autorregulado. Sin embargo, en la actualidad,

apenas es discutido que ese espacio no es independiente sino dependiente de compañías tecnológicas y programadores que se rigen por las reglas del mercado. En ese sentido, la neutralidad política de ese espacio, que continúa siendo el objetivo más o menos utópico en un Estado democrático pluralista, necesita la garantía de la actuación normativa del poder público, por más que su aplicación resulte difícil.

En puridad, el proceso ha sido similar al que se advierte en la respuesta del ordenamiento jurídico ante cualquier nuevo fenómeno. Inicialmente se pretende la autorregulación. Luego, cuando surgen los primeros problemas de naturaleza jurídica se intentan resolver a través de la aplicación analógica del Derecho vigente por parte de los distintos operadores jurídicos y, finalmente, se aborda la regulación del fenómeno no sólo a través de normas jurídicas sino también de organismos o instituciones que se ocupen se garantizar el cumplimiento de esa normativa. Lo cierto es que un marco regulador claro de la IA genera confianza tanto a los usuarios como a los propios proveedores.

3. Deben ser medidas adoptadas a nivel global, al menos a nivel europeo

En cualquier caso, no tiene demasiado sentido configurar marcos legales reguladores de la IA en el ámbito estatal para prever los distintos supuestos que puedan plantearse. Las medidas deben adoptarse a nivel global pues la actuación de las compañías tecnológicas mediadoras no se ciñe a un determinado Estado. Algunos Estados han aprobado leyes que inciden en este fenómeno. En Alemania se aprobó en 2017 una Ley federal para luchar contra el discurso de odio en las redes sociales; en Francia, se aprobaron en 2018 dos leyes de lucha contra la manipulación de la información en los distintos procesos electorales que permite al juez retirar los mensajes engañosos que afecten a los procesos electorales y hayan sido difundidos de forma masiva y automatizada o en Canadá se aprobó también en 2018 la Ley de modernización de las elecciones, que obliga a mantener un registro de las actividades publicitarias de carácter político. Sin embargo, más allá de las polémicas que estas leyes han generado en los distintos países (O. Sánchez Muñoz, 2020: 146-170), su limitación deriva de que pretenden afrontar desde lo local, desde los ordenamientos jurídicos estatales, un fenómeno global.

En efecto, la globalización, y la consecuente limitación de la efectividad del marco constitucional estatal, se manifiestan claramente en este supuesto. En cualquier caso, debemos ser conscientes de la dificultad de que se ofrezca esa respuesta global. No existen ni las instituciones, ni las estructuras, ni los procedimientos para ello. Pensar en la creación de una institución reguladora internacional cuyas actuaciones fueran respetadas por todos los actores resulta ciertamente utópico. Por ello, como mínimo, deben ofrecerse respuestas en marcos regionales y, en lo que nos afecta, en el marco europeo. En este sentido, la UE está en condiciones de ofrecer respuestas a través de su ordenamiento jurídico y de su estructura institucional. Además, ha mostrado una especial preocupación por este fenómeno. Han sido muchos los documentos elaborados en los últimos años por la Comisión Europea (Comunicación “Inteligencia Artificial en Europa” de 2018, Libro Blanco sobre IA de 2020), el Parlamento (Resoluciones sobre Ética, Responsabilidad y Derechos de propiedad intelectual de octubre de 2020) o la Agencia de Derechos Fundamentales de la Unión Europea. Fueron actos preparatorios

para la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial y se modifican determinados actos de la Unión, presentada por la Comisión Europea en abril de 2021 y, actualmente, sometida a debate. Esta regulación será directamente aplicable en todo el territorio de la UE pero el objetivo es que pueda servir de referencia y, en ese sentido, extienda su influencia a todo el mundo. En cualquier caso, como es conocido, el procedimiento legislativo europeo es largo, con una profusa negociación en las distintas instituciones, por lo que no se espera la entrada en vigor del Reglamento hasta el año 2023 como mínimo, con una moratoria para las sanciones de dos años a fin de que las organizaciones se adapten a las obligaciones de la nueva legislación.

4. Las medidas deben dirigirse también a actores privados

También resulta relevante destacar que las medidas no sólo deben dirigirse a los poderes públicos sino también a los actores privados. Las compañías tecnológicas suelen rechazar que su actuación tenga consecuencias políticas. Y, ciertamente, en la mayoría de los casos no lo pretenden pues estas compañías tecnologías viven de la publicidad y su única finalidad es el beneficio económico, al margen de las cuestiones éticas. Pero el negocio puede desarrollarse precisamente en el ámbito político, con consecuencias para los propios procesos electorales, como hemos visto en el asunto Cambridge Analytica.

En cualquier caso, no son meras plataformas de información y comunicación, que ponen a disposición del usuario, sino que al diseñar algoritmos para gestionar los datos actúan como intermediarias del proceso. De esta forma, objetivamente, esas compañías privadas inciden en el proceso político. Han ocupado buena parte del espacio público por lo que ejercen un poder que no es estrictamente privado, aunque se rijan por el derecho privado, sino que obligan a replantear las categorías de lo público y lo privado (F. Balaguer Callejón, 2022: 65). Se han convertido, por tanto, en sujeto de poder y, por ello, en objeto de regulación para limitar su actuación desde el Derecho Constitucional Europeo. La intervención en ese ámbito no debe plantear problemas de adecuación constitucional en un modelo social y democrático de Derecho.

5. El objetivo es lograr el control humano y la neutralidad de la IA a través de estructuras y procedimientos de control

Finalmente, debemos destacar que el objetivo de la regulación debe ser garantizar la intervención humana a través de un sistema de gobernanza para supervisar las actividades relacionadas con la IA. Los seres humanos que interactúan con los sistemas de IA deben mantener el control sobre estos sistemas. En este sentido, la propuesta de Reglamento europeo de IA, mencionada antes, hace hincapié en que son seres humanos quienes deben establecer los objetivos de los sistemas de IA y también quienes deben supervisar su aplicación y los resultados de ésta. A partir de ello, se podrán articular procedimientos que garanticen la neutralidad del mediador y el respeto en su actuación a los principios que rigen una sociedad democrática pluralista. En este sentido, resulta

necesario desarrollar estructuras y procedimientos que permitan un mayor control de los efectos y consecuencias de la IA.

V. LOS DERECHOS DE PARTICIPACIÓN POLÍTICA FRENTE A LA INTELIGENCIA ARTIFICIAL EN EL MARCO EUROPEO.

1. Legislar sobre Inteligencia Artificial en la Unión Europea.

A partir de las líneas tendenciales expuestas deberían concretarse las actuaciones normativas precisas para garantizar los derechos de participación política y el sistema democrático en la aplicación de sistemas de IA. Hemos dicho ya que esa regulación no puede limitarse a la modificación de la LOREG, o a la aprobación de leyes específicas contra la desinformación, como se ha experimentado en algunos países, sino que debe abordarse la regulación de la IA. Además, también hemos sostenido que esa regulación debe ser europea, no estatal; que debe alcanzar a los actores privados y garantizar el control humano a través de estructuras y procedimientos para garantizar la evaluación y control de los instrumentos de IA.

La Resolución del Parlamento Europeo de 16 de febrero de 2017 de recomendaciones destinadas a la Comisión sobre Normas de Derecho Civil sobre Robótica (2015/2103/INL) reclamaba a la Comisión un marco legal europeo sobre esta cuestión. En ese sentido, la Comunicación de la Comisión Europea, Inteligencia Artificial para Europa COM (2018) 237 final, de 25 de abril, planteaba incluir normas sectoriales de Derecho civil, laboral, etc. que aborden las situaciones derivadas de la IA, a la vez que apelaba a los Estados a "garantizar el establecimiento de un marco ético y jurídico apropiado basado en los valores de la UE y en consonancia con la Carta de Derechos Fundamentales de la UE". Sin embargo, ello suponía, de alguna forma, desentenderse de la cuestión. Es evidente que resulta necesario actualizar la legislación civil o laboral de los Estados miembros para hacer frente a las nuevas situaciones derivadas de la IA. Así, la responsabilidad civil derivada de un accidente provocado por un coche autónomo o el despido de un trabajador para ser sustituido por un robot, por poner dos ejemplos que se están planteando en la práctica, no pueden quedar sólo a la interpretación de los órganos jurisdiccionales, aplicando una normativa que ignora el fenómeno tecnológico. Sin embargo, tampoco podemos quedarnos en este tratamiento casuístico y sectorializado. Es necesario un marco regulatorio general con principios, normas de contenido y una estructura institucional para abordar la incidencia de la IA no sólo en los derechos fundamentales sino en la propia organización política de la sociedad, como hemos comprobado.

Afortunadamente, esa primera posición de la UE se ha modificado posteriormente y, en la actualidad, parece dispuesta a asumir su responsabilidad regulatoria en este ámbito. Ya hemos mencionado que en abril de 2021 la Comisión Europea presentó la propuesta de Reglamento sobre IA a fin de permitir el uso y desarrollo de los sistemas de IA de forma garantista, evitando sus riesgos y consecuencias negativas.

2. La importancia del Reglamento General de Protección de Datos para la garantía de los derechos en relación a la Inteligencia Artificial

Hace pocos años se aprobó el 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 esos datos (RGPD). En relación a nuestro objeto, ha supuesto un avance importante en la garantía de los derechos afectados por la obtención y uso de datos a través de la IA, y en concreto de los derechos de participación política. Se ha dicho que de haber estado en vigor en 2016 hubiera sido más difícil que Cambridge Analytica realizara sus actividades de influencia subliminal en los procesos electorales, al menos en Europa (O. Sánchez Muñoz, 2020: 178).

En puridad, la aprobación del Reglamento europeo ha supuesto transformar el derecho fundamental a la protección de datos de carácter personal en un derecho europeo pues queda plenamente regido por el RGPD, completado por la legislación interna sólo en los supuestos en los que la legislación europea remita a ella (A. Rallo Lombarte, 2019: 50; M. Medina Guerrero, 2022: 145). En ese sentido, estamos ante una respuesta europea que incide en la problemática que abordamos.

El primer elemento a destacar es que, en virtud del RGPD, el consentimiento del usuario para el uso de sus datos tiene que ser expreso, no basta con el consentimiento tácito. Sin duda, esto puede generar problemas de aplicación práctica pero constituye una garantía para los derechos de la ciudadanía.

Además, se incluye también una garantía fundamental a nuestro objeto cual es el principio de finalidad. Implica que los datos personales no pueden utilizarse para finalidades distintas a aquellas para las que hubieran sido recogidos, esto es, resulta necesario establecer una conexión entre la finalidad original y las finalidades ulteriores. Recordemos que en el caso Cambridge Analytica se utilizaron para el perfilado político datos obtenidos a través de un test de personalidad retribuido para un estudio académico.

No obstante, el elemento fundamental a analizar es la prohibición del tratamiento de las "categorías especiales de datos personales", entre las que se encuentran las "opiniones políticas" (art. 9.1), y sus excepciones. Las excepciones son: a) el consentimiento explícito del interesado; b) que se trate de datos hechos públicos por el interesado o c) apelando a razones de interés público esencial. Sin embargo, en puridad en este momento sólo la segunda excepción es aplicable en España.

El consentimiento explícito del interesado para el tratamiento de las categorías especiales de datos, como son los referidos a la orientación política, tiene a su vez una excepción de la excepción en el RGPD cuál es que el Derecho de la Unión o de los Estados miembros puede establecer de manera expresa que esa prohibición no pueda ser levantada por el interesado. Es lo que ocurre en España. El art. 9.1 LOPD establece de forma indubitada que "el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico".

Y tampoco resulta aplicable en España la excepción del "interés público". Es claro que el legislador europeo ha introducido un concepto jurídico indeterminado en unos términos "laxos y abiertos" (R.M. García Sanz, 2019: 132). Se ha vinculado a la posibilidad de que los partidos políticos recopilen datos personales sobre las opiniones políticas en el marco de sus actividades electorales, con las garantías adecuadas y vinculado al funcionamiento del Estado democrático. Sin embargo, hemos visto que la STC 76/2019 ha declarado inconstitucional y nula la forma en que esa excepción ha sido articulado por el legislador español, en el art. 58 bis. 1 LOREG, al no haber explicitado el interés público al que responde y no haberse establecido las "garantías adecuadas". Por tanto, aunque el Reglamento europeo es de aplicación directa, la indeterminación de esa concreta previsión normativa imposibilita su aplicación sin la intermediación del legislador nacional. Por ello, conforme a la doctrina del TC, en este momento tampoco resulta posible acudir en España al argumento del "interés público" pues el legislador tendría que establecer las circunstancias en las que puede ser invocado, la justificación de dicho tratamiento excepcional y las garantías "adecuadas y suficientes" en las que se podría producir el tratamiento (R.M. García Sanz, 2019: 136). Es cierto que de la STC 76/2019 no puede derivarse una prohibición del perfilado político (J.C. Hernández Peña, 2022: 57), sino una exigencia de concreción legislativa del interés público. Sin embargo, a partir de los riesgos del perfilado político y la microsegmentación de este tipo de mensajes con instrumentos de IA, no parece fácil vincular su utilización por los partidos políticos a un mejor funcionamiento del Estado democrático.

En consecuencia, el RGPD garantiza que los datos personales no van a ser obtenidos sin el consentimiento expreso del interesado para ser utilizados con fines políticos y también frente a la utilización con ese objeto de los obtenidos con consentimiento para otros fines. Incluso, en España ni siquiera resulta posible el consentimiento para el uso de los datos sobre orientación política y tampoco es aplicable, al menos en la actualidad, la excepción del "interés público". Sin embargo, lo que no se impide completamente, aunque se dificulte, es que a partir de las opiniones políticas manifestadas públicamente a través de las redes sociales, por ejemplo, se puedan hacer perfiles ideológicos de los usuarios y remitirles mensajes microsegmentados.

En efecto, en virtud del 9.2 e) RGPD se podrán tratar datos sin consentimiento de sus titulares cuando hayan sido hecho públicos de manera manifiesta o el 9.2 e) lo permite cuando el tratamiento se refiera a miembros actuales o antiguos de partidos políticos o a personas que mantengan contactos regulares con ellos y se lleve a cabo en el ámbito de sus actividades legítimas. De hecho, el 58 bis 2 LOREG, que no ha sido cuestionado ante el Tribunal Constitucional, permite "utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante la campaña electoral".

Además, la elaboración de perfiles no está prohibida por el RGPD pese a lo establecido en el art. 22 RGPD[2], sino sometida a unas obligaciones más estrictas al ser una forma de tratar los datos potencialmente intrusiva. Estas obligaciones se recogen en las Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los

[2] "Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar"

efectos del Reglamento 2016/679, adoptados el 3 de octubre de 2017. En ese sentido, se reconoce el derecho de oposición, se establece un tiempo máximo de mantenimiento de los perfiles, la realización de una evaluación de impacto sobre la privacidad y la intervención de un delegado de protección de datos. Además, conforme al art. 22.2 a) y c) los Estados miembros podrán determinar los supuestos en que se pueden adoptar decisiones automatizadas y las medidas adecuadas para salvaguardar los derechos e intereses legítimos del interesado, vinculado funcionalmente al sistema democrático y en el marco de actividades electorales (J.C. Hernández Peña, 2022: 53).

No obstante, si nuestro ordenamiento prohíbe incluso dar el consentimiento para el tratamiento de nuestros datos sobre orientación política, en los márgenes que abre el Reglamento europeo, es que quiere impedir el tratamiento de ese tipo de datos y, por tanto, que los partidos políticos o, especialmente, compañías privadas de comunicación política elaboren perfiles ideológicos de las personas para sacarlos al tráfico mercantil a fin de elaborar mensajes políticos microsegmentados.

En esa línea, las rendijas que aún existen en relación al tratamiento automatizado de datos personales de naturaleza política deberán ser cubiertas desde el futuro Reglamento Europeo de Inteligencia Artificial. Se trata de establecer mecanismos de supervisión permanente para las herramientas de IA a fin de impedir que con los datos circulantes sobre orientaciones políticas se puedan elaborar perfiles ideológicos individualizados de millones de personas y enviar publicidad y presunta información microsegmentada, con la intención de alterar su comportamiento electoral. Deben ser complementarias una legislación electoral que prohíba la publicidad electoral subliminal, una legislación de protección de datos que limite la obtención de datos de carácter político y una legislación de IA que supervise las herramientas para que no se haga un tratamiento de los datos legítimamente obtenidos con la intención de interferir en los procesos electorales.

3. La propuesta de Reglamento europeo de IA. La estructuración de los sistemas de IA en cuatro niveles de riesgo

La propuesta de Reglamento europeo estructura los sistemas de IA en cuatro niveles de riesgo para los derechos fundamentales, de lo que resulta la imposición de más o menos obligaciones en función de dicho riesgo.

En primer lugar, están los sistemas de IA prohibidos por conllevar un riesgo inadmisible para la seguridad o los derechos y libertades de la ciudadanía. Son aquellos capaces de manipular el comportamiento humano, predecir información respecto a determinados colectivos para identificar sus vulnerabilidades o circunstancias especiales o que impliquen la identificación biométrica o la videovigilancia masiva por parte de las autoridades en espacios públicos, aunque en estos casos se acepta bajo autorización judicial o administrativa, incluso “a posteriori” en supuestos de urgencia, lo que resulta ciertamente discutible. En estos casos, y con las excepciones mencionadas, los sistemas están directamente prohibidos por el riesgo que implican para los derechos y libertades.

En segundo lugar, encontramos los sistemas de IA de alto riesgo, a los que se dedica la mayor parte de la propuesta de Reglamento (arts. 6 a 51). Los incluidos en este listado no están prohibidos pero conllevan un alto riesgo para la salud, la seguridad o los

derechos y libertades y, en consecuencia, están sujetos a obligaciones reforzadas que garanticen su uso seguro. Son las tecnologías empleadas en infraestructuras críticas como transportes, que ponen en riesgo la vida y salud de las personas; en formación educativa o profesional, que pueden determinar el acceso a la educación; componentes de seguridad de los productos; gestión del acceso al empleo como los programas de clasificación curricular; servicios de carácter público o privado como los sistemas de calificación crediticia; gestión de migración, asilo y control de fronteras; aplicación de leyes que puedan interferir en derechos de las personas como la celebración de pruebas selectivas o sistemas aplicados a la administración de justicia y a los procesos democráticos.

Estos sistemas quedan sometidos a una evaluación de conformidad y gestión del riesgo en relación al cumplimiento de unas obligaciones específicas. En concreto, serían las siguientes: gobernanza de los datos para que mantengan estándares de calidad, ausencia de sesgos, etc.; seguridad y supervisión humana; deberes de transparencia sobre el funcionamiento del sistema; inscripción en una base de datos a nivel europeo; superación del test de conformidad y obtención de la certificación correspondiente, con unas especificaciones técnicas que habrá de cumplir.

Todas las herramientas relativas a la obtención y reutilización de datos en los procesos electorales deben incluirse en los sistemas de alto riesgo y ser sometidas a la supervisión precisa para garantizar que los mensajes políticos remitidos a través del sistema tienen un carácter expreso, no subliminal. La única referencia que encontramos en la redacción actual es la mención que se hace a las tecnologías empleadas en procesos democráticos. Merecería, sin duda, una mayor concreción en el Anexo que pueda incorporarse durante el debate abierto en la actualidad.

En cualquier caso, son sujetos obligados por la legislación todos los que intervienen en algún momento en la cadena de valor, es decir, no sólo quien ha introducido el sistema de IA en el mercado como proveedor sino todo aquel que la utiliza. Se considera proveedor a quien modifica la finalidad prevista del sistema o realiza una modificación sustancial de éste, sustituyendo, en estos casos, al proveedor inicial. Además, se atribuye a la Comisión la posibilidad de modificar las técnicas y enfoques enumerados en el Anexo (P.A. De Miguel Asensio, 2021: 3).

Por todo ello, resulta claro que las empresas de comunicación electoral que utilizan herramientas de IA deben ser supervisadas para garantizar que los datos han sido obtenidos con el consentimiento de la persona afectada y que su uso no pretende la elaboración de perfiles ideológicos de los electores para una manipulación subliminal de su comportamiento electoral. Esta actuación se produce cuando se recaban los datos para un uso distinto al electoral y se utilizan en ese ámbito. Lo ocurrido con Cambridge Analytica no es un caso aislado sino que existen cientos de empresas en todo el mundo que se dedican a reutilizar datos en campañas electorales y a las que resulta necesario supervisar.

En tercer lugar, los sistemas de IA de riesgo medio-bajo son aquellas tecnologías de menor capacidad de intrusión en la esfera privada de las personas como asistentes virtuales o chatbots, que no suponen un riesgo alto para los derechos y libertades.

En este caso, las obligaciones se vinculan a garantizar la transparencia, de forma que su funcionamiento y características sean conocidos por los usuarios.

Finalmente, en cuarto lugar, el resto de sistemas de IA no estarían sujetos a ninguna obligación, pudiendo elegir los agentes de la cadena si se someten a sistemas voluntarios de cumplimiento, como la adhesión a códigos de conducta. En principio, quedan fuera de la aplicación del Reglamento.

Los sistemas incluidos en cada uno de los niveles de riesgo se enumeran expresamente en Anexos. Este procedimiento, que pretende reforzar la seguridad jurídica, plantea el óbice de que basta con modificar alguna de las características del sistema para que no le resulten aplicables la prohibición o las obligaciones vinculadas a un determinado nivel de riesgo.

4. Una Agencia que controle los sistemas de Inteligencia Artificial

En cualquier caso, la supervisión del cumplimiento de las obligaciones establecidas para los sistemas de IA en los distintos niveles de riesgo precisa la creación de un mecanismo de gobernanza en cuanto los límites y garantías no se aplican a la tecnología en si sino a la forma en que está es utilizable con riesgo para los derechos de las personas.

La propuesta de Reglamento es imprecisa en este aspecto fundamental. Se refiere a la supervisión por parte de las autoridades de los Estados miembros y a la creación de un Comité Europeo de Inteligencia Artificial. En el ámbito nacional se designará una autoridad nacional competente. En este sentido, parece adecuada la creación de Agencias específicas en cada Estado con esa función supervisora, como se ha hecho en relación a la protección de datos de carácter personal. En el caso de España, la Ley de Presupuestos Generales para 2022 ya prevé la creación de una Agencia Española de Supervisión de la Inteligencia Artificial. No obstante, debemos ser conscientes de los problemas que en este caso plantea la descentralización de la función de control y supervisión en los Estados miembros, mayores que en el supuesto de la protección de datos de carácter personal. Los sujetos obligados por la legislación europea serán los prestadores que introducen en el mercado o ponen en servicio sistemas de IA y los usuarios de estos sistemas, tanto situados en la UE como en un tercer país cuando el resultado se utiliza en la Unión. Es difícil imaginar un sistema de IA cuyo ámbito de actuación se limite a un Estado y, por otro lado, las compañías tecnológicas más relevantes son de fuera de la UE y sus sistemas se aplican en todos los Estados. La supervisión en cada uno de ellos puede provocar contradicciones, más allá de duplicidades. En ese sentido, resulta de especial relevancia la función de coordinación que deberá desarrollar el Comité Europeo de Inteligencia Artificial, formado, según la propuesta de Reglamento, por representantes de la Comisión, un miembro de cada una de las 27 autoridades nacionales competentes y el Supervisor Europeo de Protección de Datos.

La tarea fundamental de dichos organismos será certificar la seguridad de los sistemas de IA y, específicamente, la gobernanza de datos, en función de su nivel de riesgo no sólo con carácter previo a su comercialización sino durante todo el tiempo que se

encuentre operativa para garantizar que los algoritmos no contradicen los principios de una sociedad democrática, en concreto los derechos y libertades ni en su diseño ni en su funcionamiento.

En principio, las tareas de supervisión deberán afectar a la transparencia en la actuación, a la evaluación de impacto y a la exigencia de responsabilidad.

a) Transparencia en la actuación

En primer lugar, se trata de garantizar la transparencia de su actuación tanto si son de riesgo medio/bajo como, especialmente, si son de riesgo alto, así como para detectar cuando estamos ante un sistema prohibido.

Hasta este momento, los sistemas de IA no suelen hacer público los modelos utilizados para adoptar una decisión. Esto resulta comprensible a partir de la lógica exclusivamente economicista que ha regido su desarrollo. Incluso, desde la perspectiva de la competencia en el mercado tiene sentido esa opacidad. Sin embargo, esto no resulta posible en una IA que deba respetar los principios y derechos en una sociedad democrática. En ese marco, la IA debe regirse por el principio de transparencia en el sentido de que sea conocida y comprensible cualquier decisión adoptada. Ello supone el cumplimiento de tres principios básicos: la trazabilidad, dejando constancia de los datos y los procesos que determinan la decisión del sistema, la caja negra algorítmica; la explicabilidad, en cuanto los programadores deben justificar los motivos por los que se han utilizado determinados algoritmos y, en tercer lugar, la comunicación, en cuanto debe hacerse público para conocimiento general que se está interactuando con un sistema de IA, a fin de que los seres humanos puedan oponerse (J.L. Goñi Sein, 2019: 26). La Carta de Derechos Digitales, aprobada a través de un Acuerdo de Consejo de Ministros, sin carácter normativo, reconoce estas exigencias de transparencia como derechos ante la Inteligencia Artificial (Apartado XXV). Sin embargo, hasta ahora no existe una obligación en este sentido. El RGPD establece el deber del responsable de proporcionar, y el derecho del interesado a obtener, "información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas". Sin embargo, parece claro que ello no conlleva el derecho a exigir el acceso directo al algoritmo o a su código fuente sino a lo sumo el derecho a recibir una explicación *ex ante* sobre la funcionalidad del sistema (M. Medina Guerrero, 2022: 156, 160).

Incluso, se ha llegado a sostener que esta pretensión de lograr una rendición de cuentas de las decisiones algorítmicas a instancia del afectado por el tratamiento automatizado de sus datos puede llevar a una "falacia de la transparencia" en cuanto la ciudadanía no tiene la formación suficiente para realizar esa supervisión (M. Medina Guerrero, 2022: 169). Sin embargo, ese es el marco del RGPD. Distinta debe ser la situación con las estructuras y procedimientos que deberá prever el Reglamento Europeo de Inteligencia Artificial, y las normas internas que lo desarrollen, para la gobernanza de los sistemas de IA. La Agencia de supervisión de los sistema de IA debería poder valorar las explicaciones en relación a una serie de cuestiones como el proceso de toma de decisión de los algoritmos, las alertas cuando el funcionamiento no es adecuado, los objetivos del sistema, la protección frente a sesgos o distorsiones, la garantía del respeto a la

privacidad, etc. Es evidente que el fenómeno de la utilización falaz o discriminatoria resulta habitual y, en consecuencia, la supervisión parece necesaria. Sirva de ejemplo el caso de la Comisión Nacional de la Competencia de los Mercados cuando en su Informe de supervisión del mercado peninsular de producción de energía eléctrica del año 2015 ha puesto de manifiesto que las compañías eléctricas utilizan un algoritmo en el que las ofertas más baratas resultan descartadas (J. Ponce Solé, 2019: 17).

b) Evaluación de impacto

En segundo, lugar, a partir de esos datos, la Agencia estará en condiciones de hacer una evaluación del impacto de ese determinado sistema en los derechos y libertades. En ese sentido, el modelo es el ya previsto en relación a la protección de datos en el art. 35 del RGPD. En desarrollo de esa previsión, el art. 28 de la LO 3/2018 concreta esa evaluación a los supuestos en los que el uso de los datos pudiera vulnerar derechos fundamentales o producir situaciones discriminatorias, o cuando se trata de crear perfiles personales. Sin embargo, en el supuesto de la IA esta evaluación debe configurarse como una supervisión en todos los supuestos.

Esto es fundamental en relación a los derechos de participación política pues se trata de evaluar las posibilidades de utilizar un determinado sistema de IA para incidir en el comportamiento electoral y, en este sentido, proceder a su prohibición o al establecimiento de las cautelas necesarias.

Esa evaluación de los efectos del algoritmo debe ser fundamentalmente preventiva. De poco sirve actuar cuando ya se ha producido la vulneración del derecho fundamental y la afectación del proceso electoral, más allá de exigir la responsabilidad por el daño causado. Su actuación debe regirse por el principio de precaución. En este sentido, al certificarse por la Agencia los programas de IA, los diseñadores, fabricantes y vendedores de programas deberían estar sujetos a una responsabilidad limitada de carácter extracontractual, a diferencia de si no se han sometido a dicho proceso de certificación (J.J. Vega Iracelay, 2018: 39). Pero también debe preverse la rendición de cuentas en su funcionamiento tanto de oficio como a instancias de la ciudadanía que pueda considerarse afectada por la actuación de un concreto sistema de IA.

En relación a la incidencia de los algoritmos en los procesos de participación política, hemos señalado ya que los programadores no suelen tener una específica intención política pues su orientación es económica. En el Informe elaborado por la Agencia de Derechos Fundamentales de la Unión Europea en 2021, al que se ha hecho referencia, un empresario estonio reconoce que “cuando probamos el sistema, no nos fijamos demasiado en los aspectos legales, sino en si el sistema es rentable”. Ese es el modelo de funcionamiento de la IA que debe ser modificado. Los instrumentos de IA deben ser diseñados y operados cumpliendo con los principios y los derechos fundamentales y dicho cumplimiento debe ser certificado por un organismo específico. La propia Facebook ha reconocido que es viable desde una perspectiva técnica incluir parámetros que reorienten sus algoritmos hacía determinados principios como la participación democrática y la garantía de los derechos fundamentales, aunque ello conllevaría una pérdida de ingresos. En este sentido, el control y las limitaciones podrían limitar el

progreso, más allá de reducir los beneficios económicos, pero el valor que actúa como contrapeso es más importante pues se trata de garantizar los derechos fundamentales y el propio proceso democrático.

c) Exigencia de responsabilidad

Finalmente, la supervisión y rendición de cuentas debe vincularse a la existencia de un régimen sancionador. No pueden existir espacios exentos de responsabilidad tanto jurídica como política. El robot nunca puede ser responsable. Detrás de la maquina deben identificarse personas, físicas o jurídicas, a las que pueda exigirse responsabilidad, sin perder la cadena de responsabilidad. En un sentido político, debe existir un responsable de la decisión cuando incide en el espacio público y, específicamente, en el proceso electoral. No es posible atribuir la responsabilidad al algoritmo, como se ha pretendido en relación a la distribución de refugiados en la UE. Y también debe existir una responsabilidad jurídica. Hasta ahora, la determinación de esa responsabilidad se ha trasladado de forma casuística a los órganos jurisdiccionales en un contexto conflictivo. Sin embargo, la propuesta de Reglamento europeo de Inteligencia Artificial establece un específico régimen sancionador de carácter económico, como en el RGPD o en la normativa de competencia. Se sanciona el incumplimiento relativo a prácticas prohibidas u obligaciones de gobernanza de datos en los sistemas de alto riesgo; el incumplimiento de cualquier otro requisito u obligación o el suministro de información incorrecta, incompleta o engañosa a los organismos y autoridades. Las sanciones pretenden ser a tanto alzado (30, 20 o 10 millones de euros) y también atendiendo al volumen de negocio de la empresa (6%, 4% o 2% del volumen de negocio anual a escala mundial en el ejercicio financiero anterior).

Importa destacar que no sólo pueden ser sancionados los proveedores de sistemas de IA sino todos los que intervienen en su cadena de valor. Esto es relevante en relación a la reutilización de datos personales en los procesos electorales. Y, más allá de las sanciones pecuniarias se debería prever la posibilidad de suspender una determinada actividad aunque, como cualquier actuación administrativa, resultará susceptible de control jurisdiccional.

VI. ALGUNA CONCLUSIÓN

En conclusión, sostenemos que la aprobación del Reglamento europeo de IA debería servir para reforzar la protección de los derechos de participación política y el propio proceso electoral en relación a la aplicación de la IA, permitiendo culminar la tendencia iniciada a través de la garantía del derecho a la protección de datos de carácter personal con el RGDP y la ley orgánica que lo desarrolla en España.

Es cierto que la propuesta de Reglamento no menciona la vulneración de los derechos de participación política entre los supuestos de riesgo, más que de forma implícita al referirse a los procesos democráticos. Sin embargo, ello no impide su utilización para prohibir o para condicionar aplicaciones de IA que puedan tener incidencia en el ejercicio libre, igual, directo y secreto del derecho fundamental al sufragio activo.

Y esto es así porque el futuro Reglamento no pretende regular tecnologías sino el uso que se haga de ellas *ex ante* y *ex post*. Desde el momento en que se apruebe, las autoridades de supervisión pueden solicitar a cualquier compañía documentación, archivos, etc. para comprobar que no se está incidiendo en procesos electorales.

En ese sentido, puede ser un instrumento adecuado para intentar impedir un fenómeno que ha sido limitado por la legislación electoral y la de protección de datos pero no de forma absoluta: la posibilidad de que compañías de comunicación política utilicen las plataformas tecnológicas para elaborar perfiles ideológicos de millones de electores a fin de remitirles mensajes microsegmentados, con el objetivo de influir de forma subliminal en su comportamiento electoral. Eliminar esas prácticas es una condición necesaria para garantizar un proceso electoral libre y con igualdad de armas y, en definitiva, para el funcionamiento democrático de la sociedad.

Existe el riesgo de que el control o supervisión de la IA desincentive o ralentice su desarrollo. Mark Zuckerberg sostiene que la regulación frenará el desarrollo de la IA (El País, 25 de julio de 2017). Sin embargo, los efectos negativos, de carácter fundamentalmente económico, están plenamente justificados en cuanto se trata de garantizar los derechos fundamentales y el propio sistema democrático. Supervisar, controlar y limitar la posible incidencia de la IA en los procesos electorales es necesario para que este desarrollo tecnológico no conlleve una involución democrática.

BIBLIOGRAFÍA

- Balaguer Callejón, F. (2022), *La Constitución del algoritmo*, Fundación Manuel Giménez Abad, Zaragoza.

- Bobbio, N. (2003), *Teoría General de la Política,* Trotta, Madrid.

- Castellanos Claramunt, J. (2019), "La democracia algorítmica: inteligencia artificial, democracia y participación política", *Revista General de Derecho Administrativo*, 50.

- De Miguel Asensio, P.A. (2021), "Propuesta de Reglamento sobre inteligencia artificial", *La Ley Unión Europea*, 92.

- García Sanz, R.M. (2019), "Tratamiento de datos personales de las opiniones políticas en el marco electoral: todo en interés público", *Revista de Estudios Políticos,* 183.

- Goñi Sein, J.L. (2019), "Innovaciones tecnológicas, inteligencia artificial y derechos humanos en el trabajo", *Documentación Laboral*, 117.

- Hernández Peña, J.C. (2022), "Campañas electorales, Big Data y perfilado ideológico. Aproximación a su problemática desde el derecho fundamental a la protección de datos", *Revista Española de Derecho Constitucional*, 124.

- Judt, T. (2010), *Algo va mal,* Taurus, Madrid.

- Medina Guerrero, M. (2022), "El derecho a conocer los algoritmos utilizados en la toma de decisiones. Aproximación desde la perspectiva del derecho fundamental a la protección de datos", *Teoría y Realidad Constitucional,* 49.

- Ponce Solé, J. (2019), "Inteligencia artificial, Derecho administrativo y reservad e humanidad: algoritmos y procedimiento administrativo", *Revista General de Derecho Administrativo,* 50.

- Rallo Lombarte, A. (2019), "El nuevo derecho de protección de datos", *Revista Española de Derecho Constitucional,* 116.

- Sánchez Barrilao, J.F. (2016), "El Derecho Constitucional ante la era de Ultrón: la informática y la Inteligencia Artificial como objeto constitucional", *Estudios de Derecho. Universidad de Deusto.* Vol. 64/2, julio-diciembre, 2016.

- Sánchez Muñoz, O (2020), *La regulación de las campañas electorales en la era digital,* CEPC, Madrid.

- Vega Iracelay, J.J. (2018), "Inteligencia artificial y derecho: principios y propuestas para una cogobernanza eficaz", *Informática y Derecho. Revista Iberoamericana de Derecho Informático (segunda época),* 5, segundo semestre, 2018.