RECLUTAMIENTO TECNOLÓGICO. SOBRE ALGORITMOS Y ACCESO AL EMPLEO *

María Teresa Alameda Castillo

Profesora Titular de Derecho del Trabajo y Seguridad Social
Universidad Carlos III de Madrid**

EXTRACTO **Palabras clave:** reclutamiento, algoritmo, inteligencia artificial, discriminación, protección de datos

Las nuevas tecnologías manifiestan una extraordinaria capacidad de vulneración de los derechos fundamentales y ello tiene un impacto singular en el derecho de privacidad y en el derecho de no discriminación. Si, además, la inteligencia artificial lleva a cabo operaciones de clasificación personal con criterios algorítmicos y sin intervención humana significativa, también del derecho a la dignidad humana. En el contexto de una relación de trabajo tal situación de vulnerabilidad es evidente pero más aún en el proceso de acceso a un puesto de trabajo (reclutamiento por algoritmo).

Ante ello, es preciso fijar un completo diseño de garantías que incluya gobernanza de datos, seguridad y supervisión humana y deberes de transparencia. La dimensión preventiva se acompañaría de la reparadora y habría de implicar a actores públicos, privados y sujetos colectivos en la vigilancia previa y permanente de la implementación de sistemas de inteligencia artificial en el trabajo. En definitiva, avanzar hacia la gobernanza algorítmica.

En este contexto, la Unión Europea ya ha emprendido el camino hacia el desarrollo tecnológico ético y confiable, propio del modelo europeo y en abril de 2021 presenta la propuesta de Reglamento sobre inteligencia artificial

ABSTRACT **Key words:** recruitment, algorithm, artificial intelligence, discrimination, data protection

New technologies show an extraordinary capacity to violate fundamental rights and this has a unique impact on the right to privacy and the right to non-discrimination. If, in addition, artificial intelligence carries out personal classification operations with algorithmic criteria and without significant human intervention, also the right to human dignity. In the context of an employment relationship such a situation of vulnerability is evident but even more so in the process of accessing a job (recruitment by algorithm).

Given this, it is necessary to establish a complete design of guarantees that includes data governance, security and human supervision and transparency duties. The preventive dimension would be accompanied by the reparative one and would have to involve public, private and collective actors in the prior and permanent surveillance of the implementation of artificial intelligence systems at work. In short, move towards algorithmic governance.

* Este trabajo se ha realizado en el marco del proyecto de investigación nacional Cambio tecnológico y transformación en las fuentes laborales: ley y convenio colectivo ante la disrupción digital. Agencia estatal de investigación. 2019-2021. RTI2018-094547-B-C21.

** ORCID 0000-0002-9590-6053

 Recepción original: 16.06.2021 Aceptación 13.07.2021

ÍNDICE

1. INTRODUCCIÓN

En un mundo tecnificado e hiperconectado, las nuevas tecnologías facilitan la vida y mejoran los procesos y la productividad. La máquina agiliza y, en principio, parece eliminar la subjetividad propiamente humana lo que puede redundar en innegables beneficios. En el ámbito de las relaciones de trabajo aquellas facilitan la selección de trabajadores y la gestión de los recursos humanos en el día a día de las empresas (asignación de tareas, distribución de tiempos y lugares de trabajo, evaluación y promoción profesional, consecución de objetivos, incentivos...).

Así, tanto en el acceso al empleo como en el desarrollo de la prestación de servicios, el empleador ejerce hoy un poder de dirección tecnológico que supone la participación de máquinas en el proceso de toma de decisiones (en su totalidad o en una parte del mismo). Aquí radica la novedad y también la necesidad de cautela y de fijar garantías porque, ahora, aquella máquina es un algoritmo que adopta decisiones que afectan a personas (potenciales candidatos a un empleo o trabajadores), lo que nos lleva, de partida, a su cuestionamiento desde los derechos de igualdad y no discriminación y también del derecho de privacidad (especialmente, derecho de protección de datos). Los algoritmos, no solo pueden perpetuar las desigualdades en la sociedad sino también integrarlas de manera opaca, al tiempo que se consideran objetivos y precisos (O'Neil)[1]. Además, a través del *profiling* (elaboración de perfiles) se clasifica, etiqueta a las personas y se emiten juicios de

[1] *Armas de destrucción matemática, Cómo el Big Data alimenta la desigualdad y amenaza la democracia,* Ed. Capitán Swing, 2018.

ellas hacia el futuro (podemos ser buenos para este trabajo, seremos productivos, qué parece que vamos a hacer y qué no...). Este hecho, sumerge a la sociedad en una concepción determinista que deja poco margen a la autonomía individual y al libre desarrollo de la personalidad[2].

Siguiendo con la igualdad, con carácter general, su proyección en el ámbito de las relaciones privadas es limitada pero, aquí, sí se despliega el principio de no discriminación. Esto es, el empresario habrá de evitar decisiones sesgadas que creen situaciones de discriminación lo haga con técnicas humanas o (ahora) digitales. En el ámbito del acceso al empleo, por ejemplo, el *objetivo* algoritmo habrá sido diseñado para obtener un resultado a partir de una secuenciación de pasos, pero ya aquí puede haber sesgos (sexo, edad, raza, religión...). Esto es, el código fuente del algoritmo revela su construcción sesgada que excluirá a determinados candidatos (v gr. se entrena al sistema utilizando única o principalmente datos relativos a hombres y ello se traduce en exclusión o resultados peores para las mujeres).

Pero hay más, esta sencilla operación que ahorra tiempo y costes en la selección de personal (la máquina no acusa cansancio, no hay que pagarle horas extras, puede seguir revisando CVs toda la noche o el fin de semana...)[3] es frecuente que se haga más sofisticada mediante el aprendizaje automático profundo del algoritmo (*deep learning*). No es sólo la simple búsqueda de las características deseadas y la selección de candidatos adecuados sino que aquel, a partir de su propio aprendizaje, determina las características idóneas, por repetición (si hay más CV de hombres que aplican a puestos STEM, preferirá a hombres) y por asociación (Persona de color/hispano-delincuencia, Mujer. Reducciones jornada-menos productividad-...). El sistema de IA aprende mientras está funcionando y aquí los resultados no pudieron preverse ni anticiparse en la fase de diseño sino que son las repercusiones prácticas de las correlaciones que reconozca el sistema en un gran conjunto de datos[4] (Comisión Europea), así, sus juicios se basan en predicciones matemáticas con parámetros estadísticos Por tanto, desde la óptica de la no discriminación estaríamos ante dos situaciones posibles: a) En la primera hay una discriminación directa: voluntad de excluir a determinados candidatos de una oferta de empleo. b) En la segunda, *a priori*, no existe intencionalidad

[2] Morente Parra, V., "Big Data o el arte de analizar datos masivos. Una reflexión crítica desde los derechos fundamentales", Derecho y Libertades, junio 2019, p. 21.

[3] Además, en principio, basa sus resultados en criterios objetivos (elimina la subjetividad del reclutador –que, en ocasiones, pueden tomar decisiones por afinidad personal), adapta la productividad al puesto y predice acontecimientos futuros. Ahora bien, junto a estos pros, también hay contras: la eliminación de la figura humana del reclutador, la no consideración de aptitudes ni emociones personales, la práctica clonación de candidatos reclutados o la selección con sesgos.

[4] *Libro Blanco sobre inteligencia artificial. Un enfoque orientado a la excelencia y confianza*. 2020, https://op.europa.eu/es/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1).

discriminatoria…salvo que la empresa, que conociera el impacto discriminatorio del algoritmo, lo consintiera y lo continuara utilizando.

Se plantea aquí que la persona, la organización, más próxima a la vulneración de derechos, al incumplimiento, sea la que haya de asumir las consecuencias. No basta señalar como culpable al sistema automatizado que los protagonizó[5].

Si el algoritmo puede desplegar efectos discriminatorios en todos los estadios de la relación de trabajo (y fuera de ella)[6], en la fase de acceso al empleo, su impacto vulnerador de derechos fundamentales es especialmente intenso y en esta fase centraremos nuestro estudio. Al margen de tecnología, el candidato a un empleo o participante en un proceso de selección, goza también en aquí, de la protección jurídica de los actos discriminatorios (nulidad, reparación –indemnización por daños y perjuicios-…) pero, en la práctica, ello se ve extraordinariamente dificultado por cuestiones de prueba. Esta debilidad se potencia ahora al combinar algoritmo, IA y *Big Data*[7]…a lo que hay añadir redes sociales. La IA sirve de apoyo a las redes sociales dotándolas de nuevos servicios y estas a su vez proveen de información y datos a los sistemas de IA[8]. La combinación de todo ello nos sitúa ante un escenario de potencial *discriminación algorítmica* (invisible, intensa y compleja técnicamente)[9].

[5] *When the algorithms mess up, the nearest human gets the blame*, MIT Technology Review. 28.5.2019.

[6] Recientemente, el RD Ley 2/2021, de 26 de enero, de refuerzo y consolidación de medidas sociales en defensa del empleo modifica el art. 53.1 LISOS permitiendo a la ITSS emitir actas de infracción basadas en actuaciones automatizadas, en algoritmos, esto es, sin intervención directa del personal funcionario actuante en su emisión. En relación a los cambios incorporados, Molina Navarrete sostiene que si el algoritmo de empresa puede discriminar a las personas empleadas, el algoritmo de la Administración de la Seguridad Social también puede a las empresas (o personas autónomas) fiscalizadas. De ahí que se reclame extender las garantías del Estado de derecho (transparencia, motivación accesible…) a las decisiones administrativas mediante algoritmos predictivos de eventuales fraudes a la Seguridad Social ("Duelo al sol digital. ¿Un algoritmo controla mi trabajo? Sí, a tu empresa también, Revista Trabajo y Seguridad Social CEF, nº 457, abril 2021, p. 19).

[7] El *Big Data* es una tecnología disruptiva que se vale de un nuevo tipo de análisis de datos, consistente en la identificación de patrones conductuales y, como consecuencia de ello, delimita un nuevo conocimiento sobre el individuo y posibilita su clasificación personal. Es conocido como la tecnología de las cinco v: volumen, variedad, velocidad, valor y veracidad (Morente Parra, V., "El Big Data o el arte de analizar datos masivos…, *op. cit*., p. 225.).

[8] CUATRECASAS. Instituto de Estrategia legal en RRHH. Proyecto Technos 2016-2019, *Inteligencia artificial y su impacto en los recursos humanos, en el mercado de trabajo y en el marco regulatorio de las relaciones laborales*, Ed Wolters Kluwer, Madrid, 2018.

[9] Sáez Lara, C., "Algoritmos y discriminación en el empleo: un reto para la normativa antidiscriminatoria", NREDT, nº 232, 2020, p. 4.

Así, el algoritmo se nutrirá y entrenará con datos y estos pueden ser facilitados por los propios candidatos a un empleo o no, pero igualmente utilizados en el proceso. En la búsqueda del candidato idóneo, se utilizarán datos que proceden de fuentes diversas, se interconectarán, se elaborarán perfiles y se sacarán conclusiones. Y en todo esto, ¿dónde están las garantías? ¿qué límites establece el derecho? De partida, como avanzamos, la utilización de IA y la capacidad de los algoritmos de transformar los datos sobre las características de los candidatos en predicciones sobre su desempeño futuro en el puesto de trabajo puede afectar, de un lado, a la prohibición de discriminación (art. 14 CE) y, de otro, a la protección de los datos personales (tratamiento de los datos, decisiones automatizadas, elaboración de perfiles–art. 22 RGPD[10]-). Ahora bien, estas nuevas formas de gestionar el acceso al empleo (reclutamiento tecnológico) hacen que las posibilidades lesivas de aquellos derechos fundamentales se potencien y se expandan (alcanzando, por ejemplo, a otras dimensiones del derecho de privacidad o incluso al derecho a la dignidad humana), de ahí la necesidad de que las garantías de protección que ya tenemos sean objeto de reinterpretación, ampliación y, además, y junto a ello, sean precisas otras reglas específicas (IA). Sólo con el marco de garantías presente, la protección será insuficiente ante el *efecto multiplicador* del algoritmo en la vulneración de derechos fundamentales en los procesos de selección y contratación de trabajadores: aprende de sí mismo, capta masivamente datos (de los candidatos [o incluso de aquellos que ni siquiera lo son], de características de estos), trata datos (interconecta), elabora perfiles y toma decisiones.

En los últimos años, la espectacular proyección de la IA en todos los ámbitos y, también, en el mundo del trabajo ha abierto un interesante debate sobre su impacto en los derechos humanos y la necesidad de fijar un marco de protección. En esta línea, el Consejo de Europa anima a los Estados miembros a incentivar la innovación tecnológica de acuerdo con los derechos humanos existentes, incluidos los derechos sociales y las normas laborales y de empleo reconocidas internacionalmente[11] y la Unión Europea, tras un intenso debate y acciones políticas y normativas diversas, ya ha presentado su Propuesta de Reglamento sobre Inteligencia artificial[12].

Punto de partida esencial en el documento es la afirmación de que la posibilidad de sesgo y discriminación de los programas informáticos, los algoritmos y los datos debe abordarse estableciendo normas para los procesos de diseño y uso, ya que este enfoque podría convertir a aquellos en un contrapeso considerable al sesgo y la discriminación, así como en una fuerza positiva para el cambio social. Esto es, los

[10] Reglamento 2016/679 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.

[11] Recomendación CM/Rec (2020) 1 del Comité de Ministros de los Estados miembros. *Los impactos de los sistemas algorítmicos en los derechos humanos*. 2020, https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154

[12] *Vid., infra*, 4.

algoritmos como instrumento al servicio de la no discriminación y los derechos humanos. De ahí la ambivalencia de la IA y los algoritmos que a la vez que pueden discriminar, pueden corregir la discriminación y los parámetros de actuación sesgados (IA al servicio de la diversidad)[13]. En este contexto, la *Estrategia española de IA* (2019) apunta entre las prioridades para el Gobierno español, la evitación de sesgos y prejuicios de género y otros tipos de discriminación y plantea enfocar, desde una visión multidisciplinar, el diseño general de los sistemas de IA desde un alineamiento de los aspectos éticos, legales y sociales y contribuir desde la I+D+I a la redacción de un Código ético de la IA[14].

Es imposible predecir el desarrollo tecnológico futuro pero, como expresa Merino Rus, sí podemos anticipar para qué mundo lo queremos: uno que respete la dignidad, libertad e igualdad de las personas orientando los avances en tecnología a estos principios universales o uno que los menoscabe e incluso los anule. Para dirigirnos a lo primero y no a lo segundo, la IA y los algoritmos habrán de ser justos, diseñarse y aplicarse de buena fe, ser inclusivos, confiables, explicables y auditables[15]. En esta línea, la Comisión europea perfila los rasgos de la IA confiable: acción y supervisión humanas, solidez técnica y seguridad, gestión de la privacidad y los datos, transparencia, diversidad, no discriminación y equidad, bienestar social y ambiental y rendición de cuentas. En la medida en que las máquinas están programadas para tomar decisiones de un modo lógico-matemático, puramente racional, la pérdida del *factor humano* quizá sea un lujo[16] que no nos podamos permitir perder como especie. Y ello (el *humano al frente*) es, además, una exigencia que deriva de las garantías recogidas en las normas antidiscriminatorias y de protección de datos y del proyectado marco regulador europeo de IA.

2. INTELIGENCIA ARTIFICIAL EN LOS PROCESOS DE SELECCIÓN DE PERSONAL: EL RECLUTAMIENTO POR ALGORITMO

La aplicación de la IA en los procesos de selección de personal supone concentrar en un algoritmo, a través de una secuencia puramente matemática,

[13] CUATRECASAS. Instituto de Estrategia legal en RRHH, Proyecto Technos*, Informe general. El impacto de las tecnologías disruptivas en la gestión de los recursos humanos y en el marco regulatorio de las relaciones laborales*, Ed. Wolters Kluwer, Madrid, 2019, p. 202.

[14] https://www.ciencia.gob.es/stfls/MICINN/Ciencia/Ficheros/Estrategia_Inteligencia_Artificial_IDI.pdf,

[15] *Los derechos humanos, la democracia y la igualdad en la era de los algoritmos y la Inteligencia artificial* , Asociación de Investigación por la Paz Gernika Gororatuz, Red Gernika, Doc 20, 2020, ps. 35 y 36.https://www.gernikagogoratuz.org/portfolio-item/derechos-humanos-democracia-igualdad-inteligencia-artificial-rafael-merino-rus/

[16] Martínez, "Cuestiones de ética jurídica al abordar proyectos de *Big Data*. El contexto del Reglamento general de protección de datos", Dilemata, nº 24, 2017, p. 154.

la búsqueda, selección y reclutamiento de candidatos a un empleo[17]. De partida, el filtrado de CVs y candidaturas en los procesos de selección se puede ver positivamente afectado por la IA pues se ganará en eficacia y rapidez en la criba de currículums, la automatización de la extracción de información de aquellos, o de los perfiles de redes sociales profesionales y su comparación con los requisitos del puesto ofertado, ofreciendo como resultado el conjunto de candidatos que mejor encajan y disponiendo de informes basados en la analítica de estos datos[18]. Este desplazamiento de los procesos humanos en las distintas fases de selección hacia sistemas automatizados plantea, no obstante, considerables desafíos e interrogantes. Partiendo de que la complejidad tecnológica dificulta las razones de los resultados y los hace difícilmente atacables, la apariencia de objetividad conduce a que aquellos se perciban como incuestionables[19].

Ahora bien, aun cuando la aplicación matemática viene precedida de un previo testeo con una muestra significativa que estadísticamente permite concluir su fiabilidad, su empleo ha de sujetarse también a las prevenciones de la normativa de protección de datos en lo que se refiere (entre otros extremos) al derecho a obtener una respuesta humana, o lo que es lo mismo, no confiar al cien por cien de la decisión al cálculo algorítmico[20]. Ello nos lleva platear si es posible indagar en el modelo que tomó la decisión para verificar si presenta sesgos (en su diseño o ejecución) o, lo que es lo mismo, el acceso al código fuente del algoritmo y

[17] Para la Propuesta de Reglamento, IA son sistemas informáticos que, entre otros aspectos, recopilan, tratan en interpretan datos estructurados o no estructurados, identifican patrones y establecen modelos con objeto de extraer conclusiones o tomar medidas en la dimensión física o virtual sobre la base de dichas conclusiones y algoritmos, el modelo de cálculo u otras operaciones de resolución de problemas llevadas a cabo por programas informáticos para ejecutar una tarea. Por su parte, la lesión o daño es toda lesión física, emocional, mental, sesgo, discriminación o estigmatización, sufrimiento causado por la falta de inclusión y diversidad, pérdida financiera o económica, pérdida de empleo, o de oportunidad educativa, restricción indebida de la libertad de elección, condena injusta, daño medioambiental y toda infracción del Derecho de la Unión que sea perjudicial para una persona.

[18] CUATRECASAS. Instituto de Estrategia Legal en RRHH. Proyecto Technos, *Informe general. Impacto de las tecnologías disruptivas…, op. cit.,* p. 197.

[19] El algoritmo es una tecnología intelectual que supone, en última instancia, la sustitución de juicios intuitivos por una respuesta objetivada. Un conjunto de instrucciones matemáticas, una secuencia de tareas destinada a conseguir un cálculo o resultado (Mercader Uguina, J., "Algoritmos: personas y número en el Derecho digital del trabajo", Diario La Ley 23 de febrero de 2021. https://diariolaley.laleynext.es/dll/2021/02/24/algoritmos-personas-y-numeros-en-el-derecho-digital-del-trabajo, p. 1).

[20] Rivas Vallejo, P., *La aplicación de la inteligencia artificial al trabajo y su impacto discriminatorio*, Ed. Aranzadi, Pamplona, 2020, p. 313.

aquí nos topamos con la protección de su *secretismo* como límite al derecho de transparencia. Después volveremos específicamente sobre esta cuestión[21].

En el proceso de acceso a un puesto de trabajo podemos distinguir varias fases comenzando por el diseño de la oferta, el reclutamiento de candidatos, las distintas fases de selección con técnicas diversas (tests, dinámicas de grupo, *role play*, entrevistas medias…) y la toma de decisión (después, normalmente, de una entrevista final). La presencia de la tecnología en todas ellas es ya una realidad innegable que experimentará un desarrollo exponencial en el futuro. Desde el mismo diseño y lanzamiento de la oferta es fácil localizar supuestos que, de la mano de la IA, del *Big Data* y de las redes sociales generan impacto en la no discriminación. Pensemos en estas como vía de publicación de ofertas que sólo llegan a determinados perfiles por la acción de un algoritmo (ofertas flotantes/ dirigidas. Sistema *Lookalike*) o del *branding* empresarial que permite a las empresas obtener información de los perfiles de empleados preferidos por sus clientes. Este mecanismo de detección del grado de satisfacción de los clientes que contribuye a la construcción de la reputación empresarial en internet (redes sociales, webs…), puede condicionar también la política de contratación de la empresa en base a los gustos de los clientes. Similar era la base fáctica del caso enjuiciado por la STJUE 10 julio 2008 Asunto *Firma Feyn NV*[22] en el que el alto tribunal europeo consideró discriminatoria la conducta de la empresa de no contratar extranjeros porque sus clientes rechazaban la instalación de sus puertas de seguridad por estos. Claramente, esta decisión, mediatizada por prejuicios externos, tiene las consecuencias y protección jurídica de las conductas discriminatorias (nulidad, indemnización, eventual sanción administrativa), en este caso, en el acceso al empleo[23]. Ahora bien, en el uso de sistemas digitales de reputación automatizados se podría deslizar el sesgo diluido en un criterio más genérico, el de la mejora de la prestación del servicio a los clientes, mezclado con otras variables consideradas por algoritmo en cuestión[24].

Hoy, el 95% de los departamentos de RRHH de grandes grupos y el 50% de las pequeñas y medianas empresas europeas utilizan ATS (*Applicant Tracking System*). El reclutador define el perfil del candidato con una serie de palabras clave que le gustaría encontrar en las cartas de motivación y en sus CVs. El robot escanea las candidaturas recibidas y calcula una tasa de adecuación entre la descripción de puesto y los CVs. Las candidaturas que tienen mejores evaluaciones son

[21] *Vid., infra*, 3.4.

[22] C-54/07,
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62007CJ0054&from=ES.

[23] *Vid*., Alameda Castillo, M.T., *Estadios previos al contrato y discriminación,* Ed. Aranzadi, Pamplona, 2013, págs. 303 ss.

[24] Rivas Vallejo, P., *La aplicación de la inteligencia artificial al trabajo…, op, cit.,* p. 236.

presentadas al reclutador y los candidatos que fueron rechazados en el proceso de selección reciben, de forma automática, un correo de cortesía.

Pese a la aparente objetividad del algoritmo en esta fase, se pueden producir resultados indeseables. Un ejemplo reciente es el caso Amazon. En el año 2014, la compañía comenzó a construir una herramienta con el objetivo de automatizar y optimizar las búsquedas. Se desarrolló en el centro de Ingeniería de Edimburgo y el objetivo era diseñar una IA que pudiera rastrear la web con el fin de identificar talentos para incorporar a la compañía. Fueron creados 500 modelos informáticos y los entrenaron para que reconocieran unos 50000 términos que aparecían en los CVs de candidatos que se habían presentado en los últimos 10 años. Un año después, la empresa comprobó que el software calificaba a los postulantes a los empleos técnicos con un sesgo en contra de las mujeres pues al ser hombres la mayoría de los candidatos, el algoritmo infirió que ser hombre era un requisito necesario o conveniente para puestos técnicos y terminó seleccionando recurrentemente a hombres para esos. Así, la máquina penalizaba a las mujeres con independencia de su formación y experiencia. Después, la compañía modificó el modelo para que fuera neutral pero el sesgo persistía y decidió eliminar el programa en 2017[25].

Ahora bien, también se alude a las diversas fortalezas del reclutamiento tecnológico como son su posible flexibilidad, de un lado, y su capacidad para localizar perfiles muy especializados y escasos, de otro. En cuanto a lo primero, en el diseño del algoritmo se podría optar, por ejemplo, si no queremos perder ninguna candidatura idónea, por permitir un determinado porcentaje de ajuste (v gr. 70%) y nos incluirá perfiles que no se ajusten del todo pero se acerquen, con el objetivo de no dejar fuera ninguna candidatura potencialmente idónea. Viceversa, si establecemos un modelo que descarte a todos aquellos que no se ajusten al 100%, corremos el riesgo de excluir del proceso algún perfil válido, pero tendremos la certeza de que los que sean incluidos tendrán un grado de ajuste completo respecto a lo que estamos buscando. Por otro lado, determinados trabajos o profesiones -en relación a los cuales existe carencia de profesionales en el mercado- es especialmente adecuada la captación por IA, como las relacionadas con la transformación digital y la evolución estratégica de la tecnología (desarrollador de programas y de plataformas de conversación, analista de mercados, consultor de ciberseguridad...).

Existen otros muchos ejemplos de aplicación de algoritmos en el proceso de acceso a un empleo como los sistemas de gamificación y ludificación o la entrevista digital. En estos, a través de *killer questions* el sistema expulsa a candidatos al puesto ante respuestas no deseadas o bien a través de sistemas gamificados en línea (v gr. *juegos de Knack*) se persigue la valoración de aspectos no detectables en una entrevista personal como la intolerancia a la frustración o la incertidumbre[26]. En

[25] Rivas Vallejo, P., *La aplicación de la inteligencia artificial al trabajo…, op, cit.,* p. 232.

[26] Rivas Vallejo, P., *La aplicación de la inteligencia artificial al trabajo…, op, cit.,* p. 244.

otras ocasiones, estos juegos online pretenden captar conductas, valores y aptitudes del candidato que, junto a la entrevista, también en línea, determinará quien acudirá presencialmente a las pruebas en la empresa. Por su parte, en la entrevista digital existen sistemas como el de la empresa de software británica *Cognisess* que desarrolló un programa que detecta los talentos adecuados para las empresas. El software recepciona un video que debe ser enviado por los candidatos a un sitio web hablando frente a la cámara sobre sus expectativas y antecedentes y si bien no se descartan procedimientos tradicionales como las evaluaciones psicotécnicas, quien decidirá finalmente quien es apto o no es la máquina. El algoritmo puede analizar las expresiones faciales fugaces en el vídeo, con la posibilidad de detectar emociones básicas.

3. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN EL ACCESO AL EMPLEO Y ALGORITMOS APLICADOS AL RECLUTAMIENTO Y SELECCIÓN DE CANDIDATOS

Los algoritmos se alimentan de datos y las posibilidades de análisis de macrodatos (*Big Data*), la IA y el aprendizaje automático permiten reelaborar gran cantidad de informaciones simples, de forma que, combinadas entre sí a través de técnicas estadísticas y lógicas, es posible determinar, analizar, predecir ciertos aspectos de la personalidad o el comportamiento, los intereses y los hábitos de una persona[27]. Así, de la misma forma que algoritmos seleccionan para nosotros, tendencias, posibilidades de ocio, información, por pistas o sesgos que hemos dejado en la red, intervienen en el reclutamiento y seleccionan candidatos con datos *esparcidos* en ella...Y la acumulación masiva y el cruce de datos de demandantes de empleo y candidatos y su tratamiento, aplicando algoritmos que se basan en los referidos modelos de aprendizaje automático, podría arrojar como resultado las exclusiones apriorísticas de personas con las competencias profesionales requeridas[28] en base a otras circunstancias, discriminatorias o no.

3.1. Tratamiento de datos, redes sociales

Hoy, las empresas tienen en cuenta el perfil digital de los candidatos en los procesos de selección sea de cuentas generalistas o específicas[29]. El rastro o huella

[27] Mercader Uguina, J., "Algoritmos: personas y número en el Derecho digital del trabajo", *op. cit.,* p. 1.

[28] Olarte Encabo, S., "La aplicación de inteligencia artificial a los procesos de selección de personal y ofertas de empleo: Impacto sobre el derecho a la no discriminación", DL, nº 100, 2020, p. 81.

[29] Las redes generalistas son aquellas en las que la interacción con los usuarios no tiene vocación definida sino que busca un espacio abierto a diversos usos mientras que las redes específicas

que dejamos en las redes va delimitando nuestro perfil o marca personal que luego puede ser objeto de consideración y también de exclusión en procesos de selección y contratación. La reputación online es objeto de valoración por los reclutadores. Como evidencia el *V Informe Infoempleo-Adecco sobre Redes sociales y Mercado de trabajo*[30]*, e*l 86% de las empresas consulta las redes sociales de los candidatos preseleccionados antes de tomar una decisión de contratación, el 31% de las organizaciones ha desestimado la candidatura de algún aspirante a un puesto de trabajo por la imagen que proyecta en alguno de sus perfiles en redes y el 55% de los profesionales de RRHH encuestados reconsideró su decisión de contratación después de consultar los perfiles en redes de algún candidato preseleccionado; el 36% lo hizo empeorando su decisión. Algunos ejemplos, palabras malsonantes e insultantes, ortografía y gramática, referencia al consumo de alcohol o drogas o su promoción, contenidos sexuales o poco apropiados, afiliación sindical y política, experiencias con armas, datos que contradigan los recogido en el CV del candidato, comentarios negativos sobre empleadores o compañeros de trabajo... Asimismo, se valora la comunidad online del candidato: capacidad de relacionarse con otras personas del sector profesional (si ya se está o se ha estado empleado), proactividad, calidad de los contenidos publicados.

Pero, ¿se puede acceder a la información de las redes sociales de los candidatos? Parece que sí cuando las redes sean de acceso público y no restringido (privado). Ahora bien, esa información son datos objeto de tratamiento y aquí entra en juego la protección del RGPD y de la LOPDPyGDD[31]. Por tanto, habrá que respetar los principios de calidad y minimización de datos y los datos habrán de

tienen perfiles de usuarios predefinidos, como las redes profesionales, de ocio o de difusión del conocimiento (Tarabini Castellani Aznar, M., "Redes sociales del trabajador, protección de datos y acceso al empleo", en AA.VV., (E. Monreal Brinsvaerd, X. Thibaut Aranda, A. Jurado Segovia), *Derecho del Trabajo y nuevas tecnologías. Estudios en homenaje al Prof. Pérez de Los Cobos en su 25ª aniversario como Catedrático de Derecho del Trabajo,* Ed. Tirant lo Blanch, Valencia 2020, ps. 256 y 257).

[30] El informe se basa en una muestra de 9.532 candidatos y de 295 profesionales de Recursos Humanos. https://www.adeccorientaempleo.com/wp-content/uploads/2017/02/Informe-2017-Empleo-y-Redes-Infoempleo-Adecco-2.pdf, p. 38.

[31] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de derechos digitales.

ser los estrictamente necesarios de acuerdo con la finalidad legítima perseguida[32] -adecuados, pertinentes y limitados[33].

Así, en las fases de reclutamiento y selección de candidatos, la finalidad legítima es valorar la capacidad profesional del candidato y para que el tratamiento sea lícito, los empleadores han de cumplir unos requisitos: a) considerar si el perfil del candidato en las redes es privado o público, b) recabar y tratar únicamente si es necesario y relevante para el desarrollo del puesto ofertado, c) suprimir los datos personales tan pronto como el candidato sea descartado o rechace la oferta, d) que el interesado sea informado de dicho tratamiento de datos antes de que participe en el proceso de selección (Goñi Sein)[34].

En definitiva, en un proceso de selección, es posible captar y utilizar los datos de un candidato publicados en redes sociales dentro de este marco de información contextual e igualmente, se podría rechazar a un candidato en base a esa información, siempre que no se base en causas discriminatorias. Es lógico admitir el interés del empresario en conocer a los candidatos a un puesto de trabajo en lo que respecta a su capacidad profesional pero es inadmisible su intromisión en aspectos y circunstancias personales que nada tienen que ver con la actividad a ejecutar[35], aun cuando ahora las redes sociales permitan un acceso fácil a aquella información y una lesión de derecho de privacidad de candidatos a un empleo.

Es evidente que en el contexto tecnológico en el que vivimos, cuando nuestra manera de relacionarnos se mueve en ámbitos digitales y la vida personal y

[32] En todo caso, el tratamiento por parte de la empresa o mediador en el empleo, de los datos personales de los trabajadores procedentes de sus cuentas o perfiles en las redes sociales, deberá sujetarse a los principios que deben regir el tratamiento (art. 5 RGPD): a) licitud, lealtad y transparencia del tratamiento, b) limitación de la finalidad, es decir, datos recogidos con fines determinados, explícitos y legítimos y no serán tratados ulteriormente de manera incompatible con dichos fines, c) minimización de los datos, pues deben ser estos adecuados, pertinentes y limitados a lo necesario en relación a los fines para los que son tratados, d) exactitud y, además, deberán adoptarse para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos, e) limitación del plazo de conservación -no más tiempo del necesario para los fines del tratamiento de los datos personales, f) tratados con integridad y confidencialidad, de tal manera que se garantice la seguridad adecuada de los mismos.

[33] Grupo del Trabajo del art. 29 (en adelante, GT29) -hoy Comité Europeo de protección de datos, *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679* - https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf).

[34] *La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa,* Ed. Bomarzo, Albacete, 2018, p. 68.

[35] De Vicente Pachés, F., "Acoso y discriminación en el trabajo a través de dispositivos tecnológicos o digitales: su incidencia en la fase de selección y acceso al empleo", en AA.VV (S. Ruanos Albertos), *Nuevas formas de acceso al empleo*, Ed. Atelier, Barcelona, 2019, p. 218 y p. 219.

profesional se proyecta y expone ante millones de potenciales usuarios de redes desarticulamos en parte el derecho a la intimidad. Este derecho se configura como un derecho defensivo, de protección frente a injerencias por parte de otro o como pretensión de exclusión de cualquier forma de conocimiento intrusivo y de divulgación. Claramente no es el derecho que opera cuando el propio usuario de la red lleva a cabo actuaciones en el seno de la misma que permiten el conocimiento de dichas esferas personales. De ahí que la configuración como canal abierto o semiabierto de comunicación de la red social, en la mayoría de sus usos, va a determinar qué derechos le son aplicables[36] dentro del amplio marco del derecho de privacidad.

Así, en primer lugar, el derecho que vela por los usuarios que interactúan en las redes sociales es el derecho a la protección de datos personales. Este derecho fundamental autónomo vinculado a la privacidad, ampara a todos aquellos datos que identifiquen o permitan identificar a una persona[37], es el derecho fundamental al control sobre los propios datos (derecho a la autodeterminación informativa o libertad informática –art. 18.4 CE–) y garantiza a los individuos un poder de disposición sobre los datos personales que han sido revelados o expuestos. El derecho de protección de datos, también alcanza a aquellos datos personales públicos que puedan ser accesibles al conocimiento de cualquiera pero que no escapan al poder de disposición del afectado e integra el derecho a decidir cuáles de esos datos proporcionar a un tercero o cuáles puede ese tercero recabar, permitiendo también al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso[38]. Ahora bien, también habría margen para el derecho a la intimidad respecto de los contenidos que aquel haya reservado al conocimiento de unos pocos ante su divulgación (si es red privada o limitada a un círculo cerrado y determinado de personas)[39]. Por ello, en el marco de este trabajo, no sería lícito por

[36] Tarabini Castellani Aznar, M., "Redes sociales del trabajador, protección de datos y acceso al empleo", *op. cit.,* p. 257.

[37] Como expresa la STC 292/2000, de 30 de noviembre, el hecho de ser datos de carácter personal no puede identificarse con datos relativos a la vida privada o íntima de las personas porque el ámbito de la protección de datos es mucho más amplio y alcanza a todo dato que permita la identificación de una persona pudiendo servir para elaborar un perfil ideológico, racial, sexual, económico o de cualquier otro tipo o que sirva a cualquier utilidad que, en determinadas circunstancias, constituya una amenaza para el individuo. En esta línea, expresará Cruz Villalón que el derecho de protección de datos se proyecta sobre cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros puede afectar a sus derechos, sean o no fundamentales (*Protección de datos personales del trabajador en el proceso de contratación: facultades y límites de la actuación del empleador*, Ed. Bomarzo, Albacete, 2019, ps. 10-11).

[38] STC 292/2000, de 30 de noviembre y 29/2013, de 11 de febrero. Tarabini Castellani Aznar, M., "Redes sociales del trabajador, protección de datos..., *op. cit*., ps. 258.

[39] Como recuerda Mercader Uguina, el derecho a la intimidad y el derecho a la protección de datos no tienen que ir necesariamente unidos. En ocasiones, determinados actos o hechos pueden

no existir fundamento jurídico alguno, solicitar las contraseñas de redes sociales a los candidatos (*shoulder surfing*) o solicitar amistad o petición de seguimiento pues, en estos casos, se produciría una intromisión ilegítima en la esfera privada de aquellos[40]. Además, habría que referir otra dimensión del derecho de privacidad que podría verse afectada, el derecho al secreto de comunicaciones, cuando en el marco de las dichas redes sociales, se utiliza la aplicación de mensajería (canal cerrado y bilateral).

Cabría cuestionar aquí, además, el tema del consentimiento. El tratamiento de datos de carácter personal puede llevarse a cabo si es necesario para la adopción de medidas precontractuales a instancia del interesado (art. 6.1.b] RGPD). Así, es admisible con fines de empleo y, entre ellos, se incluye el reclutamiento de los trabajadores en el que aquel tratamiento no requerirá consentimiento pero sí información, en los términos de los art. 13 RGPD y del art. 11 LOPDPyGDD. En este precepto se establece la obligación del responsable del tratamiento de aportar la información básica (identidad del responsable del tratamiento, finalidad del mismo y posibilidad de ejercer los derechos recogidos en los arts. 15 a 22 del Reglamento) y de indicar una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. En el párrafo segundo de este art. 11 se establece, además, que si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá esta circunstancia y el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho conforme a lo previsto en el art. 22 del RGPD. Por tanto, habrían de aplicarse las garantías allí establecidas[41].

Ahora bien, ¿qué ocurre cuando los datos estén en redes sociales en relación a las cuales se ha expresado un consentimiento genérico?[42] Pues, claramente, ello

ser constitutivos de vulneración a uno y no de otro al tratarse de categorías diferentes (*Protección de datos personales y garantía de los derechos digitales en las relaciones laborales,* Ed Francis Lefebvre, Madrid, 2019, 3ª edición, p. 23 y p. 24).

[40] En este sentido, Talens Visconti, E., *Incidencia de las redes sociales en el ámbito laboral y en la práctica procesal,* Ed Francis Lefebvre, Madrid, 2020, p. 30 y Fernández Fernández, R., *Redes sociales y Derecho del Trabajo. El lento tránsito desde la indiferencia legislativa a la necesaria regulación legal o convencional*, Ed. Aranzadi, Pamplona, 2021, p. 86. También, *Dictamen GT29 2/2017 sobre el tratamiento de datos en el trabajo* (17/ES. WP 249) y *Recomendación CM/Rec (2015)5 del Comité de Ministros del Consejo de Europa* que señala que el empleador debería evitar solicitar acceso a aquella información que los candidatos compartan online, especialmente en redes sociales. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a

[41] *Vid., infra,* 3.2.

[42] En el caso de red de carácter abierto, se localizan pronunciamientos judiciales que mantienen una renuncia voluntaria tácita a la privacidad (STSJ Asturias 14.6.2013 [Rº 241/2013] y STSJ Galicia 25.4.2013 [Rº 5998/2012]).

no legitimaría el tratamiento de datos *captados* que nada tuvieran que ver con la capacidad profesional del participante en un proceso de selección y, en relación a estos, además, habrían de cumplirse las reglas generales de finalidad, calidad de los datos (mínimos, pertinentes, necesarios) y el derecho de información al que acabamos de aludir (en este caso, art. 14 RGPD)[43]. En esta línea, la *Recomendación CM/Rec (2015)5 del Comité de Ministros del Consejo de Europa* en referencia al tratamiento de datos personales de las personas físicas en el ámbito laboral[44], entiende que los datos personales recopilados por los empleadores con fines de empleo deben ser relevantes y no excesivos, dado el tipo de empleo y las necesidades de información del empleador[45]. También para el GT29 (*Dictamen 2/*2017) los empresarios no deben asumir que simplemente porque el perfil de una persona en las redes sociales es de acceso público, está permitido que traten esos datos para sus propios fines pues para ello se requeriría un fundamento como es el interés legítimo. Además –como acabamos de referir- los empresarios solo podrán recoger y tratar datos personales relativos a los solicitantes de empleo en la medida en que la recopilación sea necesaria y pertinente para el puesto. Por ejemplo, el empresario podría tener la base jurídica necesaria -interés legítimo, condición de licitud del tratamiento-[46] para revisar la información de acceso público relativa a los candidatos si fuera preciso evaluar los riesgos específicos de estos respecto de una función específica y están correctamente informados (v gr. en el texto de la oferta de trabajo)[47]. Además, podría haber supuestos excepcionales (empresas de tendencia y para puestos de tendencia) en los que fuera necesario revisar la información de acceso público relativa a los candidatos en relación con las opiniones políticas, las convicciones religiosas. Por su parte, si se tratara de datos extraídos de redes profesionales, la situación sería distinta porque, precisamente, la presencia en las

[43] En esta línea también, Méndez, V., "Redes sociales y procesos de selección", Actualidad Jurídica Aranzadi, nº 937, 2018, p. 12 y Rodríguez Escanciano, S., *Derechos laborales digitales: garantías e interrogantes,* Ed. Aranzadi, Pamplona, 2019, p. 208.

[44] Esta recomendación pretende unificar el tratamiento y control de los riesgos que la exposición actual a las nuevas tecnologías y los medios de comunicación electrónica plantea en cuanto a la defensa de los derechos y libertades fundamentales de los trabajadores.

[45] Afirma también que los datos de los candidatos deberían eliminarse en el momento en que se tome la decisión de no contratarlos (aunque será posible conservarlos para futuras convocatorias si se advierte de ello y se permite a los candidatos solicitar la cancelación de sus datos en cualquier momento).

[46] Tarabini Castellani Aznar, M., "Redes sociales del trabajador, protección de datos y acceso al empleo", *op. cit.,* ps. 266-267. También, Mercader Uguina, *Protección de datos y garantía de los derechos digitales en las relaciones laborales,* Ed. Francis Lefebvre, Madrid, 2019, 3ª edición, p. 91.

[47] *Dictamen GT29 2/2017 sobre el tratamiento de datos en el trabajo,* cit.

mismas ya tiene una connotación profesional[48]. En estas, el profesional, de manera voluntaria proporciona aquellos datos que estima relevantes a esos efectos.

Al margen de estas particulares consideraciones para redes profesionales y para determinados trabajos, la posibilidad y realidad de captación de datos en redes se potencia y amplía cuando en el proceso intervienen algoritmos que, precisamente, tienen su fortaleza en localizar datos de muy distinta naturaleza, de fuentes diversas y seleccionar los candidatos más idóneos, lo que supone, además emitir decisiones predictivas[49].

3.2. Decisiones automatizadas y elaboración de perfiles

El art. 22 RGPD establece (no así la Ley española) la prohibición general de las decisiones basadas únicamente en tratamiento automatizado. Esto es, el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles[50], que produzca efectos jurídicos en él (individuo) o le afecte de modo similar y que no se basarán en las categorías especiales de datos, salvo que medie consentimiento o puedan aducirse razones de un interés público esencial, con las cautelas sobre el mismo expresadas en el RGPD y siempre que se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado. Ello supone, como expresa el GT29, que en las decisiones automatizadas los datos han de ser tratados de manera leal, lícita y transparente pues la elaboración puede ser desleal y generar discriminación, por ejemplo, al denegar a las personas el acceso a oportunidades de empleo[51].

Por tanto, hay una prohibición general de decisiones individualizadas basadas únicamente en tratamiento automatizado pero aquellas dos excepciones

[48] En Alemania, la Ley Facebook permite a los empresarios consultar los datos de candidatos recogidos en redes sociales profesionales (LinkedIn, Xing...) y los contenidos en redes sociales generalistas (Facebook, Twitter, Myspace...).

[49] Olarte Encabo, S., "La aplicación de inteligencia artificial a los procesos de selección de personal…, *op. cit.,* p. 82.

[50] El art. 4.4 RGPD define la elaboración de perfiles como toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física. Aun cuando la referencia normativa conjunta a decisiones automatizas y a elaboración de perfiles sea frecuente y ello pueda conducir a pensar que siempre han de ir juntas, puede no ser así. Esto es, pueden llevarse a cabo decisiones automatizas con o sin elaboración de perfiles y la elaboración de perfiles puede darse sin realizar decisiones automatizadas.

[51] *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679,* cit., p. 12.

(autorización por ley y consentimiento explícito del interesado) se acompañan de otra especialmente importante en el ámbito que estamos tratando. Se trata de los supuestos en los que sea necesario para la celebración o la ejecución de un contrato y, así, serían posibles las decisiones individuales exclusivamente automatizadas y la elaboración de perfiles a efectos de contratación pero aquí, el *criterio de necesidad* será requisito de licitud[52]. Además, el art. 22 se aplicará a las decisiones únicamente automatizadas parciales o previas (elaboración de perfiles) y a las finales y definitivas, pero siempre que produzcan efectos jurídicos o afecten significativamente de modo similar a la persona interesada. Así, como ya ha sido precisado doctrinalmente, esa afectación jurídica o significativa a los interesados de las decisiones automatizadas, es otra pieza clave del precepto. Claramente, las decisiones automatizadas y la elaboración de perfiles en el acceso al empleo entrarían aquí y, con frecuencia, se cumpliría con el requisito de necesidad (volumen de datos, personal afectado). No obstante, si no fuera así, las decisiones automatizadas sólo podrían actuar como colaboradores de los responsables empresariales, que analizarán la información procesada y, podrían incluso, modificar la decisión automatizada[53].

Dejamos a un lado esta última reflexión y seguimos con aquellos supuestos de autorización excepcional de decisiones totalmente automatizadas. En ellas, el responsable del tratamiento asume la obligación de adoptar medidas adecuadas para salvaguardar los derechos, libertades e intereses legítimos de los interesados y ello incluye, el derecho a obtener intervención humana, junto con la posibilidad de expresar el punto de vista e impugnar la decisión. Esta intervención, para no ser ficticia, ha de consistir en una labor de supervisión real y significativa y llevarse a cabo por persona autorizada y competente para modificar –en su caso- la decisión tomada por medios automatizados, teniendo en cuenta todos los datos pertinentes[54]. El GT29 concreta, en estos supuestos que suponen excepciones al régimen general, el cumplimiento de las obligaciones de transparencia: a) informar al afectado de que se está llevando a cabo esa actividad, b) aportar información significativa sobre la lógica aplicable, c) explicar la importancia y las consecuencias previstas del tratamiento. Además, los datos habrán de ser tratados conforme a los principios generales expuestos, habrá que minimizarlos y tener capacidad para explicar

[52] En esta línea Baz Rodríguez, J., *Privacidad y protección de datos de los trabajadores en el entorno digital* Ed. Wolters Kluwer, Madrid, 2019, p. 326. También, Mercader Uguina que sostiene que la necesidad implica que no se pueden adoptar métodos menos intrusivos para la privacidad -v. gr el volumen de candidaturas es muy elevado- (*Protección de datos y garantía de derechos digitales*..., *op. cit.,* p. 100).

[53] Sáez Lara, C., "Algoritmos y discriminación en el empleo..., *op. cit.,* ps. 10 y 11.

[54] Baz Rodríguez, J.*, Privacidad y protección de datos de los trabajadores en el entorno digital..., op. cit.,* p. 325. También, *Adecuación al RGPD de tratamientos que incorporan inteligencia artificial*, febrero 2020, https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf, p. 28.

y justificar la necesidad de su recopilación y mantenimiento, siendo necesario, por su parte, asegurar la exactitud de los datos en todas las fases del proceso y compatibilizar -en su caso- el tratamiento ulterior con la finalidad original para la que se recopilaron datos (v gr. cuando se consiga el empleo).

A esto habría que añadir, conforme al art. 35 RGPD, que será necesaria evaluación del impacto de protección de datos (EIPD) cuando se lleve a cabo una evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar (apartado. 3.a]). Esto es, cualquier decisión automatizada, incluida la elaboración de perfiles, y con independencia de que están basadas únicamente en tratamiento automatizados de datos o de si concurre intervención humana decisora[55]. La EIPD ha de estar documentada y cuando se evidencia un alto riesgo residual, ha de someterse a la autoridad de control (en las condiciones establecidas en el arts. 36 RGPD). Además, ha de concretarse en la adopción de una serie de medidas específicas y concretas para la gestión del riesgo orientadas a reforzar las obligaciones de cumplimiento[56].

Se englobaría tal actuación en la responsabilidad proactiva, en línea con las afirmaciones de la AEPD en relación a las estrategias de trasparencia, gestión del riesgo y mecanismos de auditoría y certificación que permitan el cumplimiento de las disposiciones del RGPD y mejoren la confianza de los usuarios en productos y servicios basados en IA. El RGPD no establece de forma específica qué elementos de responsabilidad proactiva hay que implementar de forma obligatoria o la forma de implementarlos, limitándose a proporcionar un amplio grado de flexibilidad para que distintos tratamientos se adecúen a la norma. Sin embargo, sí establece que dichas medidas se han de seleccionar siguiendo un análisis basado en el riesgo (RBT) y específicamente en el riesgo para los derechos y libertades de las personas con relación al tratamiento de sus datos personales y la elaboración de perfiles. Y entre estos riesgos, el más característico es el que se deriva del sesgo en los sistemas de toma de decisiones sobre las personas o su discriminación (*algorithmic discrimination)* [57].

En el ámbito interno, también contiene previsiones en la línea arriba expuesta, la *Carta de derechos digitales*[58] que dentro de los derechos en el ámbito laboral

[55] Sáez Lara, C., "Algoritmos y discriminación en el empleo: un reto..., p. 10.

[56] Aedp, *Adecuación al RGPD de tratamientos que incorporan inteligencia artificial*, febrero 2020, p. 32-33-

[57] AEPD, *Adecuación al RGPD de tratamientos que incorporan inteligencia artificial*, febrero 2020, p. 30.

[58] Desde el Ministerio de Asuntos Económicos y Transformación Digital se ha elaborado la *Carta de Derechos Digitales de España*, uno de los compromisos fundamentales del plan España

(XVII.4) establece que sin perjuicio del derecho a no ser objeto de una decisión basada únicamente en procesos de decisión automatizada –salvo en los supuestos previstos en la ley- se informará a los representantes de los trabajadores y a las personas directamente afectadas sobre el uso de la analítica de datos o sistema de IA en la gestión, monitorización o procesos de toma de decisión en materia de recursos humanos y relaciones laborales. Este deber de información alcanzará, como mínimo, al conocimiento de los datos que se utilizan para alimentar los algoritmos, su lógica de funcionamiento y a la evaluación de resultados. Además, cuando se empleen procedimientos de IA que produzcan efectos jurídicos en las personas o les afecten significativamente se reconocen los derechos a solicitar supervisión e intervención humana y a impugnar la decisión (Derechos ante la IA. XXIII.2).

3.3. Una recapitulación de garantías desde la protección de datos, un apunte desde la no discriminación y la posible proyección a la Inteligencia artificial

En materia de selección y contratación de trabajadores, a la luz de la normativa de protección de datos y en relación a las decisiones automatizadas y a la elaboración de perfiles, el RGPD y el GT29 establecen garantías ligadas a la obligación de transparencia del responsable del tratamiento. En particular, este derecho de información se concreta, cuando el tratamiento implique la toma de decisiones basada en la elaboración de perfiles (independientemente de si entran en el ámbito de las disposiciones del artículo 22), en la aclaración de que el tratamiento tiene fines tanto de elaboración de perfiles como de adopción de una decisión sobre la base del perfil generado[59]. Si se trata de decisiones únicamente automatizadas, la obligación de informar de la decisión totalmente automatizada y el supuesto excepcional en el que se fundamenta aquella, dada la prohibición general del art. 22 RGPD (celebración de contrato), el derecho a obtener una intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión. En línea similar la AEPD precisará que si el tratamiento incluye la elaboración de perfiles o decisiones automatizadas, habrá que informar claramente que se

Digital 2025. En el proceso se ha contado con numerosas contribuciones de la sociedad civil, así como el trabajo de un grupo de expertos. El borrador de la Carta se sometió a consulta pública hasta el 21 enero 2021 y recoge un conjunto de principios y derechos para guiar futuros proyectos normativos y el desarrollo de las políticas públicas de forma que se garantice la protección de los derechos individuales y colectivos en los nuevos escenarios digitales. Reconoce el derecho a la igualdad en los entornos digitales, la no discriminación y la no exclusión y, además, en los procedimientos de transformación digital se aplicará la perspectiva de género.https://www.mptfp.gob.es/portal/funcionpublica/secretaria-general-de-funcion-publica/Actualidad/2020/11/2020-11-19.html

[59] Grupo Trabajo del art. 29 de la Directiva *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*. 17/ES. WP251rev.01, 2017 (revisión 2018), p. 18.

produce esta circunstancia, de su derecho a oponerse a la adopción de decisiones individuales automatizadas de acuerdo con el art. 22 RGPD, de la información significativa sobre la lógica aplicada y de la importancia y las consecuencias previstas de dicho tratamiento para el interesado[60]. Junto a ello -como acabamos de indicar-, en todo caso, siempre que la empresa acuda a un sistema automatizado para la contratación de trabajadores deberá realizar la EIPD[61].

Como expresión de transparencia, el derecho a la explicación, habrá de ser suficiente sobre cómo funciona un algoritmo sin revelar el secreto empresarial que lo protege –después desarrollaremos algo más esta cuestión- (*vid. infra*). En palabras de Rivas Vallejo, sin facilitar información sobre el diseño técnico o informático del mismo, se puede compartir una explicación funcional en lenguaje común para que cualquier persona interesada, sin los conocimientos técnicos suficientes, pueda entender bajo qué parámetros ha podido ser afectado por un modelo matemático de decisión[62]. Todo ello (y sin perjuicio de los derechos y acciones de defensa colectivas) serían elementos para fundamentar una eventual demanda por discriminación algorítmica en el derecho a la igualdad de oportunidades en el acceso al empleo[63].

¿Y qué ocurriría ante la negativa a aportar aquella información o si esta no fuera suficiente? Es interesante traer a colación aquí la STJUE 19.4.2012 Asunto *Galina Meister*[64], en la que el tribunal europeo, aun partiendo de la consideración de que de las Directivas de igualdad de trato (Directivas 2000/43/CE, 2000/78/CE y 2006/54/CE) no se deriva un derecho a acceder a la información relativa a si al término del proceso de selección el empresario ha contratado a otro candidato, matiza que la negativa empresarial a ofrecer esta información al aquel, que de forma verosímil reúne las condiciones enunciadas en el anuncio de contratación y cuya candidatura ha sido rechazada, genera efectos en la tutela antidiscriminatoria pues tal denegación, se puede considerar un indicio de que la decisión empresarial

[60] Además, como otra manifestación de transparencia, los responsables deben proporcionar a los interesados, información sobre los mecanismos que les permita solicitar intervención humana en la evaluación o cuestionar la decisión tomada por el sistema de forma automática, más allá de lo estrictamente establecido en los artículos 13 y 14 del RGPD (*Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial,* cit., p. 23 y 34).

[61] Sáez Lara, C., "Algoritmos y discriminación en el empleo: un reto..., p. 12.

[62] *La aplicación de la inteligencia artificial al trabajo..., op. cit*., p. 327.

[63] Olarte Encabo, S., "La aplicación de inteligencia artificial a los procesos de selección de personal..., *op. cit.,* p. 82.

[64] C-415/10. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62010CJ0415&from=es

consistente en la no contratación se ha producido por motivos discriminatorios (en ese caso se alegaba sexo, edad y origen racial)[65].

Cabría plantear aquí la oportunidad de aplicar esta garantía en los procesos de reclutamiento tecnológico a través de algoritmos reforzando las reglas en materia de prueba del Proceso de tutela de derecho fundamentales y libertades públicas (arts. 177-184 LRJS). En esta línea, la rúbrica XXV de la *Carta de los derechos digitales* tras declarar que todas las personas tienen derecho a la tutela administrativa y judicial de sus derechos en los entornos digitales afirma que los poderes públicos evaluarán las leyes administrativas y procesales vigentes a fin de examinar su adecuación al entorno digital y propondrán, en su caso, las reformas oportunas en garantía de los derechos digitales.

Al margen de ello y expuesta la protección vigente desde la protección de datos, la irrupción de la IA en el ejercicio de las potestades derivados del poder de dirección lleva a cuestionarse si no podrá producirse una colisión con aquellos principios generales o, lo que es lo mismo, si la implantación intensiva de aquella en la organización del trabajo no desafía a la actual normativa de protección de datos[66] (licitud, lealtad, transparencia, limitación de finalidad, minimización, exactitud, limitación del plazo de conservación y derecho de información)[67]. Así, por ejemplo, en relación a la minimización de los datos, no deberán de ser excesivos y habrán de recopilarse solo en la cantidad mínima necesaria para la finalidad para la que se recogen lo cual choca con el carácter expansivo del algoritmo y el uso de cantidades masivas de datos de muy diversas fuentes (*big data*). Algo similar ocurre con la limitación de la finalidad, con el principio de calidad y con los períodos de conservación de los datos. Junto a ello se plantea que el actual marco regulador

[65] De esta forma, la sentencia parece avanzar una suerte de potestad o facultad de información del candidato presuntamente discriminado sin perfilar, sin embargo, su alcance y la potencial afectación de derechos de otros candidatos -protección de datos, intimidad- (Alameda Castillo, M.T., *Estadios previos al contrato y discriminación*, *op. cit.,* p. 329 y Carrizosa Prieto, E., "La concreción de los indicios de discriminación en la Jurisprudencia comunitaria", AS, nº 51, 2012, BIB 2012/3057).

En cualquier caso, la sentencia de 2012 supone un avance respecto de posicionamientos judiciales anteriores como el contenido en la STSUE 21.7.2011 *Asunto Kelly.* C-104/10 que afirmaría la no existencia de un derecho del candidato a un puesto de trabajo a recibir información sobre el proceso de selección (razones de contratación de otros candidatos ante estimación de discriminación por razón de sexo, edad, origen étnico).

[66] Se plantea ya, si el marco de obligaciones que incorpora el RGPD y la L0 3/2018 no debería ser evaluado y programado en su cumplimiento como consecuencia de los saltos cuantitativos y cualitativos que se producen con la aplicación de la IA en todo el proceso productivo y sobre la persona del trabajador (CUATRECASAS. Instituto de Estrategia legal en RRHH. Proyecto Technos 2016-2019, *Inteligencia artificial. Impacto en la organización del trabajo...,* p. 26 e *Informe general. Impacto de las tecnologías disruptivas en la gestión de los recursos humanos,* p. 212).

[67] Arts. 5, 13 y 14 RGPD.

de los datos personales es una herramienta insuficiente e incompleta frente a los datos de entrenamiento del algoritmo que son anónimos o están anonimizados y, además, el sesgo podría producirse de forma espontánea por el propio aprendizaje progresivo que el algoritmo realiza automáticamente[68].

Pese a la reciente entrada en vigor de la actual normativa de protección de datos, se cuestiona si esta no ha envejecido ya, de manera prematura, como consecuencia de la presencia disruptiva de la IA en el mercado de trabajo. La propia Comisión europea en el *Libro Blanco sobre IA* precisa que será necesario adaptar la normativa sobre empleo (Directivas antidiscriminatorias) y ello nos lleva a plantearnos la necesidad de reforzar las garantías (en una dimensión proactiva y reactiva)[69] amén de la que disciplina la protección de datos. En esta línea afirmará Rivas Vallejo que el RGPD ha perdido vigencia y capacidad para absorber la complejidad del uso de la IA[70] y ello pese a que la Propuesta de reglamento sobre IA recuerda la plena aplicación del RGPD y su carácter complementario a las futuras normas sobre IA.

Llegados a este punto cabría plantearse si las propias garantías de la protección de datos no podrían servir de base, exportarse o inspirar el uso ético y confiable de la IA. No en vano las reglas que hoy tenemos sobre decisiones automatizadas y elaboración de perfiles, tratamientos típicos de sistemas de IA, están en las normas de protección de datos. La respuesta, por tanto, ha de ser afirmativa[71]. La propia AEDP se sitúa en esta línea como refleja su documento *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción* (febrero 2020)[72]. Entiende la Agencia que el empleo de estrategias de transparencia, gestión del riesgo y mecanismos de auditoria y certificación no sólo permitirán el cumplimiento de lo establecido en el RGPD, sino que mejorarán la confianza de los usuarios en los productos y servicios basados en IA. Será, además, una actividad continuada a lo largo de todo el ciclo de vida de los sistemas de IA que exigen vigilancia sobre la legitimidad ética de sus tratamientos y sobre los posibles efectos inesperados en su funcionamiento[73].

[68] Rivas Vallejo, P., *La aplicación de la inteligencia artificial al trabajo..., op. cit.,* p. 406.

[69] *Vid., infra,* 5.

[70] Rivas Vallejo, P., *La aplicación de la inteligencia artificial en el trabajo..., op. cit.,* p. 296.

[71] En esta línea, sostiene Sáez Lara que, en el contexto de la IA, las exigencias del estándar de regulación del RGPD, constituyen un modelo para la normativa antidiscriminatoria ("El algoritmo como protagonista de la relación laboral. Un análisis desde la perspectiva de la prohibición de discriminación", TL, nº 155, 2020, p. 58).

[72] https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf.

[73] Para la AEPD se abriría también un nuevo mercado en este sector de actividad: ingenieros de privacidad, auditores, esquemas de certificación, profesionales acreditados, etc. https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf., p. 7

3.4. Perfilando el derecho de transparencia frente al algoritmo

Las garantías expuestas las trasladamos ahora a las decisiones automatizadas adoptadas por algoritmos y el derecho de transparencia frente a ellos supone que la persona interesada debe poder obtener información sobre el mecanismo que ha llevado a la conclusión que le afecta y la decisión que le perjudica[74] (información significativa sobre la lógica aplicada). Como expone el Consejo Económico y Social europeo, esa transparencia no consiste en revelar códigos, sino en hacer inteligibles los parámetros y criterios de las decisiones que se toman[75]. En esta línea el reciente RD Ley 9/2021, de 11 de mayo[76] (conocido como *Ley riders*) establece el derecho de los representantes de los trabajadores de ser informados por la empresa de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de IA que afecten a la toma de decisiones que pueden incidir en las condiciones de trabajo, el acceso y el mantenimiento del empleo, incluida la elaboración de perfiles[77]. Por su parte, en la Propuesta de reglamento sobre IA, para los sistemas de alto riesgo –entre los que se incluyen los utilizados en la selección de trabajadores-, se exige transparencia suficiente –no trasparencia total- y la obligación de aportación de información clara y adecuada a los usuarios y medidas de supervisión humana apropiadas para minimizar riesgos[78]. También en esta línea, la *Recomendación del Consejo OCDE sobre IA* recoge entre sus principios la exigencia de que los sistemas de IA sean transparentes y claros, de manera que permitan a sus usuarios entender su funcionamiento y resultados[79].

Pero ¿hasta dónde llega esa información que articula el derecho de transparencia del interesado y, también de los representantes de los trabajadores? Revisamos a continuación los límites desde normas internas y comunitarias que parecen proteger el acceso al código fuente del algoritmo. Desde las normas de la Unión Europea:

- El Considerando 63 RGPD establece que el derecho de protección de datos no debe afectar negativamente a los derechos y libertades de terceros, incluidos los comerciales o la propiedad intelectual y, en particular, los derechos de propiedad intelectual que protegen programas informáticos.

[74] Rivas Vallejo, P., *La aplicación de la inteligencia artificial al trabajo..., op. cit.,* p. 313.

[75] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv%3AOJ.C_.2018.440.01.0001.01.SPA&toc=OJ%3AC%3A2018%3A440%3ATOC

[76] Por el que se modifica el texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por RD Legislativo 2/2015, de 23 de octubre, para garantizar los derechos laborales de las personas dedicadas al reparto en el ámbito de las plataformas digitales.

[77] *Vid. infra,* 6.

[78] *Vid*., con más detalle, *infra* 4.

[79] Adoptada el 22 mayo 2019 por 42 países. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449?_ga=2.267309259.451607837.1621959205-2025991329.1621959204

Así, en base al Reglamento, podría negarse el acceso al código fuente de un eventual algoritmo utilizado en un proceso de selección y contratación de trabajadores en caso de reclamación de personas interesadas[80].

- Conforme a la Directiva 2009/24/CE, sobre la protección jurídica de los programas de ordenador[81] no pueden acogerse a la protección de los derechos de autor (Considerando 11) "*las ideas y principios implícitos en los elementos del programa, incluidas las de sus interfaces*" y tampoco lo estarán "*la lógica, los algoritmos y los lenguajes de programación que abarquen ideas y principios"*. Pese a que esta declaración excluiría la protección de los algoritmos por la vía de los derechos de autor, la STJUE 22.12.2010 Asunto *Bezpecnostni softwarová asociase* entendió que la combinación matemática a la que llamamos algoritmo sí constituye una creación intelectual, la que se documenta y escribe en lenguaje de código. Así el objeto de protección conferida por la Directiva abarcaría el programa de ordenador en todas sus formas de expresión, que permiten reproducirlo en diferentes lenguajes informáticos, tales como el código fuente y el código objeto[82]. Avanzando en esta línea, la Directiva sí ampararía una protección indirecta del algoritmo, cuando pueda plasmarse por escrito, ya que la norma extiende la protección a toda la documentación técnica y los manuales de uso de un programa, donde puede recogerse el citado algoritmo[83] (STJUE 2.4.2012 Asunto *SAS Institute Inc. v World Programming Ltd*) [84].

A nivel interno, se descarta la protección de los algoritmos por la vía de la propiedad industrial (Ley de Patentes), presenta dificultades de protección por la vía de los derechos de autor (Ley de Propiedad intelectual) y puede reconducirse, cumpliendo algunos requisitos, a la protección dispensada por los secretos comerciales (Ley Secretos empresariales):

- En relación a las patentes (art. 4.1 de la Ley 24/2015, de 24 de julio, de Patentes) se requieren tres requisitos: novedad, actividad inventiva, y aplicación industrial. Estas podrían ser características predicables de los algoritmos pero el apartado cuarto de este artículo recoge una serie de supuestos excluidos de la protección que ofrece la patente por no ser considerados invención y, entre ellos, están los métodos matemáticos.

[80] Rivas Vallejo, P., *La aplicación de la inteligencia artificial al trabajo..., op. cit.,* p. 305.

[81] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32009L0024&-from=ES

[82] Rivas Vallejo, P., *La aplicación de la inteligencia artificial al trabajo..., op. cit.,* p. 316.

[83] Economist & Jurist, *Protección legal de los algoritmos,* https://www.economistjurist.es/articulos-juridicos-destacados/proteccion-legal-de-los-algoritmos/. 8.10.2018.

[84] https://eu.vlex.com/vid/judgment-of-the-court-838782369?from_fbt=1&forw=go&fbt=webapp_preview

También, el art. 52 del Convenio sobre Concesión de Patentes Europeas[85] excluye en su apartado 2 "*a) los descubrimientos, las teorías científicas y los métodos matemáticos; (...) c) (...) así como los programas de ordenador*". Ello ha servido de base a la Oficina Europea de Patentes (OEP) para denegar las solicitudes presentadas para patentar algoritmos[86].

- El RD Legislativo 1/1996, de 12 de abril (Ley de Propiedad Intelectual) descarta la protección bajo derechos de autor de "*las ideas y principios en los que se basan cualquiera de los elementos de un programa de ordenador incluidos los que sirven de fundamento a sus interfaces*". Por tanto, la protección de los algoritmos desde el ámbito de los derechos de autor se encuentra imposibilitada de forma directa. No obstante, como acabamos de ver, la jurisprudencia comunitaria sí incorpora márgenes de protección (*vid. supra*).

- Y llegamos a los secretos empresariales. Los algoritmos, como elementos de *know-how*, pueden gozar de la protección que confiere la Ley 1/2019, de 20 de febrero de 2019, de secretos empresariales que transpone la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas. Para ello, el algoritmo deberá tener la consideración de secreto empresarial. Será este cualquier información, relativa a cualquier ámbito de la empresa, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero, que reúna tres condiciones fundamentales: a) que sea secreta, en el sentido de no ser generalmente conocida ni de fácil acceso para los círculos en que normalmente se utilizaría, b) que tenga valor empresarial como consecuencia de su carácter secreto y c) que se hayan adoptado medidas razonables por parte de su titular para que permanezca secreto. De esta forma, para que exista un secreto protegible no es suficiente con que el titular de la información aduzca simplemente que ella es secreta o confidencial sino que es necesario que efectivamente lo sea y que su revelación produzca perjuicios económicos o merme las ventajas competitivas de su titular[87]. Algunos ejemplos de

[85] Convenio de Munich sobre Concesión de Patentes Europeas, 5.10.1973 (versión consolidada tras la entrada en vigor del Acta de revisión de 29.11.2000). https://www.oepm.es/es/propiedad_industrial/Normativa/normas_sobre_proteccion_de_invenciones/Derecho_europeo_de_patentes/Convenio_de_Munich_sobre_Concesion_de_Patentes_Europeas.html

[86] Economist & Jurist, *Protección legal de los algoritmos,* cit.

[87] Azuaje, M., "El dilema de la transparencia algorítmica y los secretos empresariales", ADefinitivas. Compartimos Derecho, AD 78/2020, https://adefinitivas.com/adefinitivas-internacional/el-dilema-de-la-transparencia-algoritmica-y-los-secretos-empresariales-a-cargo-de-michelle-azuaje/

prácticas para mantener seguro el secreto serían limitar el acceso a la información relevante, encriptar los ficheros o archivos que puedan tener información sensible, desarrollar políticas de empresa para regular el acceso a ficheros o firmar acuerdos de confidencialidad con aquellas personas que pudieran gozar de un acceso directo a la información especialmente sensible. El algoritmo como secreto empresarial gozará de una naturaleza patrimonial, será objeto de derecho de propiedad por parte de su titular, que podrá transmitirlo o licenciarlo y toda apropiación, revelación o utilización realizada sin su consentimiento o incumpliendo los pactos por los que se permitió su uso o acceso, se considerará una violación de secreto empresarial ilícita con la consiguiente obligación de reparación de los daños y perjuicios causados (art. 10 Ley 1/2019).

En definitiva, el acceso al algoritmo goza de la protección de los secretos empresariales y opera como un límite al derecho de transparencia pero, en el actual contexto de desarrollo tecnológico y de avance de la IA y el *Big Data*, esto puede derivar en situaciones desequilibradas, injustas o resultar lesivo de derechos que gozan del máximo rango de protección constitucional como el derecho a la no discriminación y el derecho a la protección de datos personales. De ahí la necesidad de aumentar los niveles de acceso y transparencia[88] y avanzar en el marco de garantías a nivel privado (individual y colectivo) y a nivel público[89]. En esta línea, los controles previos y la posibilidad de realización de auditorías de los algoritmos, serían especialmente adecuadas en la medida en que, sin revelar la propia fórmula, se someterían sus resultados a control, para evidenciar si subyace un comportamiento contrario al ordenamiento jurídico[90].

- La Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública, y buen gobierno no se aplica a los trabajadores en el contexto de una relación de trabajo o a candidatos a un empleo pues es una herramienta al servicio de la transparencia de las características principales del funcionamiento de los algoritmos que pueden esgrimir los administrados ante la Administración Pública. En relación a esta norma, en fechas recientes, el Ministerio de Transición ecológica se ha negado a liberar el código fuente del Programa BOSCO que otorga o deniega el derecho a recibir la ayuda del bono social de la luz en línea con la resolución del Consejo de Transparencia y buen Gobierno de 4 de septiembre de 2019. Esta respuesta limita extraordinariamente la posibilidad de que los ciudadanos comprueben si se ha producido arbitrariedad en la toma de decisiones y fue

[88] Azuaje, M., "El dilema de la transparencia algorítmica y los secretos empresariales", cit.

[89] *Vid. infra,* 5 y 6.

[90] Berrenechea, G., "El algoritmo como secreto industrial y su control de legalidad", Legaltoday, https://www.legaltoday.com/opinion/articulos-de-opinion/el-algoritmo-como-secreto-empresarial-y-su-control-de-legalidad-2020-12-30/, 30.12.2020.

objeto de recurso contencioso-administrativo interpuesto por la Fundación CIVIO[91].

4. MARCO DE PROTECCIÓN EN INTELIGENCIA ARTIFICIAL, DÓNDE ESTAMOS Y HACIA DÓNDE CAMINAMOS. LA RESPUESTA EUROPEA: PROPUESTA DE REGLAMENTO EUROPEO SOBRE INTELIGENCIA ARTIFICIAL (2021)

Las instituciones comunitarias han facilitado e intensificado durante los últimos años la cooperación en materia de IA en toda la UE para impulsar su competitividad y garantizar la confianza sobre la base de sus valores. En la UE, la ventaja competitiva será la unión de progreso tecnocientífico y liderazgo ético[92], en definitiva, un uso ético de la IA. Como expresa ADSUARA, los derechos humanos no son un límite a la innovación sino que le dan sentido[93]. Tras la publicación de la *Estrategia europea sobre la IA* en 2018 y previa consulta de las partes interesadas, la Comisión formuló en 2019 unas *Directrices* éticas para *una IA fiable*[94] y una lista de evaluación para 2020. No buscaba sustituir la formulación de líneas de actuación político-normativa en materia de IA sino simplemente enmarcar la discusión sobre IA confiable (*Trustworthly IA*) para Europa. Se trata de generar un clima de confianza social en la IA (en el plano individual y colectivo, como base de la cohesión social)[95]. Este IA confiable se centra en el respeto por la autonomía humana, la prevención de daños, la equidad, y la capacidad explicativa.

[91] https://civio.es/novedades/2020/09/03/codigo-fuente-radar-covid-transparencia-bono-social/, 3.9.2021.
La Abogacía del Estado presentaría como prueba Informe pericial del Centro Criptográfico Nacional en el que se afirmaba que se emplean procesos de calidad en la revisión del código fuente para evitar su vulnerabilidad (que a su vez puede ocasionar un impacto severo en distintos ámbitos, como la seguridad pública o la propia seguridad jurídica de los administrados) lo que se lleva con terceros de confianza independientes. Ello ofrece, según el informe, garantías razonables (Rivas Vallejo, P., *La aplicación de la inteligencia artificial al trabajo..., op. cit.,* 347-354).

[92] Cortina, A., "Ética de la inteligencia artificial desde Europa", *El país,* 6 junio 2019.

[93] *Las empresas aplauden que se regule la inteligencia artificial, pero alertan de su coste,* https://cincodias.elpais.com/cincodias/2021/04/25/companias/1619371227_719934.html, 24.4.2021.

[94] https://op.europa.eu/es/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1

[95] Baz Rodríguez, J., *Privacidad y protección de datos de los trabajadores en el entorno digital*, Ed. Bosh, Wolters Kluwer, Madrid, 2019, p. 294.

Paralelamente, en diciembre de 2018 se publicó el primer *Plan coordinado sobre la IA*[96] como compromiso conjunto con los Estados miembros y el Consejo Económico y Social Europeo publicaría diversos dictámenes relativos al impacto social de la IA, asumiendo el compromiso, como representantes de la sociedad civil europea, de estructurar, centralizar e impulsar un debate en la materia en el que intervinieran todas las partes interesadas. En el Dictamen *Inteligencia artificial: anticipar su impacto en el trabajo para garantizar una transición justa* (2018)[97], recoge su posicionamiento en la materia. Parte de la afirmación de que los sesgos de los algoritmos, los datos de entrenamiento y los posibles efectos perversos de discriminación siguen siendo controvertidos pues, para unos, los programas informáticos de contratación predictivos podrían reducir las discriminaciones en la contratación y favorecer la contratación de los objetivamente mejores y, para otros, los algoritmos de contratación siempre pueden reflejar sesgos de los programadores y de los robots-contratadores. Por ello, es necesario velar porque sea posible un recurso humano en relación con el principio de transparencia: derecho a solicitar los criterios de decisión y por qué la recogida de los datos y su tratamiento, que habrán de responder a los principios de proporcionalidad y finalidad. Y, en todos los casos, los datos solo podrían utilizarse para los fines para os que han sido recogidos.

Por su parte, la Comisión, en *Libro Blanco sobre la IA. Un enfoque europeo orientado a la excelencia y la confianza,* publicado en 2020[98], expondría una visión clara de la IA en Europa: un ecosistema de excelencia y confianza que sienta las bases de la Propuesta de reglamento 2021. La consulta pública sobre el Libro Blanco contó con una amplia participación e iba acompañado de un «*Informe sobre las implicaciones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica*». La Comisión Europea ha presentado (21 abril 2021) su Propuesta de reglamento para regular el uso de la IA[99]. En palabras de Margrethe Vestager[100] en materia de IA *«…la confianza es una necesidad, no un lujo. Con estas normas históricas, la UE encabeza el desarrollo de nuevas normas mundiales para garantizar que se pueda confiar en la IA (...). Además, al establecer los estándares [del sector] podemos allanar el camino hacia la tecnología ética en todo el mundo y garantizar que la UE siga siendo competitiva*". La Comisión europea aspira a fijar unos estándares

[96] https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0795&from=DA

[97] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018IE1473&from=ES

[98] https://op.europa.eu/es/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1

[99] EUROPEAN COMMISSION, *Proposal for a Regulation of the European Parliament and the Council, Laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative Act* (Brussels, 21.4.2021 COM [2021] 206 final 2021/0106 [COD]).

[100] Vicepresidenta ejecutiva responsable de la cartera de una Europa Adaptada a la Era Digital.

internacionales en el sector de la IA, como ya hizo en materia de protección de datos y lograr una posición de liderazgo mundial. Reconoce que esta tecnología tiene un enorme potencial en ámbitos tan diversos como la salud, el transporte, la energía, la agricultura, el turismo o la ciberseguridad pero también entraña riesgos que pueden amenazar la seguridad de las personas y los derechos fundamentales; precisamente cita como ejemplos la opacidad de muchos algoritmos utilizados en los ámbitos de la contratación, la asistencia sanitaria o la aplicación de la ley. Por eso, ante el rápido desarrollo de la misma se quieren establecer reglas que fomenten una IA *«centrada en el ser humano, sostenible, segura, inclusiva y fiable»*.

En este sentido, el *Libro Blanco sobre IA* ya definiría previamente cuáles habrían de ser las líneas de la futura normativa europea en la materia que debería exigir a los datos de entrenamiento y a su registro y entrada, garantías de respeto a los derechos fundamentales que constituyen el pilar social de la UE. Entre otros, requisitos que garanticen que los sistemas de IA se entrenan con conjuntos de datos amplios que sean suficientemente representativos, especialmente para garantizar que todas las dimensiones de género, etnicidad y otras posibles razones de discriminación ilícita queden correctamente reflejadas en esos conjuntos de datos. También requisitos destinados a garantizar que la privacidad y la protección de datos están adecuadamente protegidos mientras se usan los productos y servicios basados en IA con arreglo al RGPD.

Siguiendo con la Propuesta de reglamento sobre IA, cuando esta se apruebe, se aplicará de forma directa a todos los Estados miembros y a todos los actores públicos y privados, tanto dentro como fuera de la UE, cuando los sistemas de IA estén ubicados en ella o su utilización afecte a ciudadanos que residen en los 27. Así, podrá afectar tanto a los proveedores (v gr. una empresa que desarrolle una herramienta de evaluación de CV) como a usuarios de sistemas de IA de alto riesgo (por ejemplo, un banco que compre esa herramienta). La normativa no se aplica, sin embargo, a los usos privados no profesionales.

La IA se define en el Propuesta de Reglamento como un software que, a partir del uso de técnicas matemáticas y de programación que se enumeran en el Anexo I (lo que se conocen como algoritmos) produce resultados que sirven para realizar predicciones, recomendaciones de decisiones futuras. La idea de partida es la necesidad de minimizar los riesgos que produce una actividad a la que no se puede o no se quiere renunciar (la misma de casi cualquier otra regulación de actividades de riesgo, por ejemplo, las industriales). A partir de aquí, se pueden utilizar varios instrumentos o técnicas de intervención: la prohibición total o parcial de ciertas actividades para evitar los riesgos (siguiendo el principio de precaución), un régimen autorizatorio (control preventivo), otras formas de control preventivo (declaraciones responsables, por ejemplo), un control exclusivamente posterior (responsabilidad civil y, en su caso, penal de quien causa daños utilizando esa técnica creadora de riesgos), todo ello acompañado de un aparato inspector, que actúa, normalmente, a instancia de los perjudicados y que ayuda a estos y a

los tribunales a descubrir y acreditar las conductas infractoras. En la Propuesta de reglamento se combinan esos enfoques, que además se adaptan a la especialidad y complejidad del objeto de regulación[101].

Las nuevas reglas se han elaborado basándose en el nivel de riesgo y la Propuesta de reglamento establece cuatro categorías: *riesgo inadmisible*, *alto riesgo*, *riesgo limitado* y *riesgo mínimo*[102]. Los sistemas de IA incluidos en la primera serán prohibidos, pues se consideran una clara amenaza para la seguridad, los medios de subsistencia y los derechos de las personas. Esto abarca los sistemas o las aplicaciones de IA que manipulan el comportamiento humano para eludir la voluntad de los usuarios (por ejemplo, juguetes que utilicen asistencia vocal para incitar a comportamientos peligrosos a los menores) y sistemas que permitan la *puntuación social* por parte de Gobiernos. Los de *alto riesgo* estarán sometidos a una serie de obligaciones muy estrictas antes de que puedan comercializarse y abarcan las tecnologías de IA empleadas en infraestructuras críticas como el transporte (que pueden poner en peligro la vida), sistemas utilizados para filtrar los CV de candidatos en procedimientos de contratación, que pueden discriminar, o sistemas de calificación crediticia que pueden impedir que una persona obtenga un préstamo[103].

Ahora bien, dentro de este grupo, hay niveles. Un primer nivel sería el de aplicaciones de alto riesgo que sirven para la identificación biométrica

[101] Huergo Lora, A., El proyecto de Reglamento sobre la Inteligencia Artificial,

https://almacendederecho.org/el-proyecto-de-reglamento-sobre-la-inteligencia-artificial, p. 1.

[102] En el caso de sistemas de IA de *riesgo limitado*, se exigen obligaciones específicas de transparencia (v gr. en los robots conversacionales, los usuarios deberán ser conscientes de que están interactuando con una máquina para poder tomar una decisión informada de continuar o no). Por su parte, para los de riesgo mínimo o nulo, la Propuesta permite el uso gratuito de tales aplicaciones (videojuegos basados en la IA o filtros de correo basura) y no interviene aquí, ya que estos sistemas de IA solo representan un riesgo mínimo o nulo para los derechos o la seguridad de los ciudadanos.

[103] En detalle, IA aplicadas en infraestructuras críticas (por ejemplo, transportes), que pueden poner en peligro la vida y la salud de los ciudadanos; formación educativa o profesional, que pueden determinar el acceso a la educación y la carrera profesional de una persona (por ejemplo, puntuación en exámenes); componentes de seguridad de los productos (por ejemplo, aplicación de IA en cirugía asistida por robots); empleo, gestión de trabajadores y acceso al trabajo por cuenta ajena (por ejemplo, sistema de IA procesos de selección o clasificación de CV para procedimientos de contratación); servicios públicos y privados esenciales (por ejemplo, sistemas de calificación crediticia que priven a los ciudadanos de la oportunidad de obtener un préstamo); aplicación de las leyes, que pueden interferir con los derechos fundamentales de las personas (por ejemplo, evaluación de la fiabilidad de las pruebas); gestión de la migración, el asilo y el control de las fronteras (por ejemplo, comprobación de la autenticidad de los documentos de viaje), administración de justiciay procesos democráticos (por ejemplo, aplicación de la ley a un conjunto concreto de hechos).

(videovigilancia con identificación de sujetos) y para el funcionamiento de infraestructuras críticas[104]. Para estas se exige verificación previa por un tercero independiente[105]. El segundo nivel es el de aquellas aplicaciones típicas de la IA predictiva, como las que sirven para determinar la admisión (o no) de estudiantes a centros educativos, la contratación de trabajadores o su promoción dentro de la empresa, la concesión -o denegación- de créditos, la concesión de prestaciones sociales (y la vigilancia sobre el cumplimiento de sus condiciones)[106]. Aquí, cada fabricante o diseñador tendrá que establecer, en cada producto de IA y en su proceso de creación y aplicación, una serie de medidas dirigidas a cumplir suficientemente los requisitos establecidos en los arts. 8-12 de la Propuesta y documentarlo. Esas medidas no serán las mismas en todos los casos, sino que tendrán que ser proporcionales al tipo de aplicación, a su complejidad, a los daños que pueda causar, al riesgo de que tales daños se produzcan…[107].

Dentro de este grupo de las aplicaciones de alto riesgo, en los dos niveles se concretan obligaciones gobernanza de datos, seguridad y supervisión humana y deberes de transparencia[108]. En concreto, aquellas habrán de estar basadas en datos de alta calidad, representativos, libres de errores y completos (art. 8). Es preciso documentar y archivar los datos generados en la creación y utilización de la aplicación (art. 9), que debe estar bien hecha y ser fiable («S*olidez, exactitud y seguridad*», art. 12), quedar siempre sometida a la dirección humana (art.11, que entre otras cosas prohíbe que el sistema pueda rechazar la intervención humana o saltarse los mecanismos de seguridad establecidos en la aplicación) y tener un grado de transparencia *suficiente* (art- 10). No se exige una transparencia total,

[104] Sistemas que controlan una central energética o de abastecimiento de agua, por ejemplo y cuyo mal funcionamiento, o ataque malicioso, podrían causar daños muy graves.

[105] Para estos supuestos en los que la Propuesta exige que la conformidad sea certificada por un tercero (aplicaciones de IA que se utilizan en productos sometidos a normativa de seguridad, las de identificación biométrica y las de manejo y control de infraestructuras críticas), se regulan las entidades de verificación en términos similares a otros sectores: entidades que son independientes de las empresas cuyos productos verifican, y que están sometidas a regulación administrativa, además de tener un seguro de responsabilidad y disponer de competencias técnicas suficientes. Sus decisiones deberán estar sujetas a recurso (art. 29).

[106] También la *policía predictiva* y la evaluación de riesgos que se utiliza para distribuir los recursos policiales o las aplicaciones de IA dirigidas a su uso por jueces y tribunales.

[107] Hay algunos casos en los que sí se establecen normas que traducen los requisitos generales en estándares concretos y la Propuesta hace referencia a ellas (IA que se aplique en productos que tienen normas de seguridad que se extiendan también a aquella -vehículos de transporte- o cuando la UE apruebe estándares técnicos sobre algún aspecto de la IA).

[108] Las aplicaciones que no estén calificadas como de alto riesgo (las probabilidades de que con ellas se causen daños a derechos o bienes protegidos son menores) podrán asumir códigos de conducta voluntarios para dar cumplimiento a los requisitos establecidos para las aplicaciones de alto riesgo.

sino compatible «*con el cumplimiento de las obligaciones legales del usuario y del proveedor»* (art. 10.1), incluidas, lógicamente, las de respetar los secretos industriales utilizados en la propia aplicación, a los que se hace expresa referencia el art. 62.1. Como ya indicamos previamente, la regulación de la transparencia es una de las cuestiones más delicadas en materia de derechos frente a la IA y la Propuesta busca un equilibrio entre aquella y los derechos comerciales/empresariales que protegen la propiedad del algoritmo. En base a ello, el proveedor debe mostrar cómo funciona la aplicación, incluida su lógica general, así como los presupuestos de partida o una descripción de los datos que se hayan utilizado para su creación, pero no se le exige transparencia total sobre el *software* utilizado[109].

En definitiva, todos estos sistemas de alto riesgo, entre los que se incluyen aquellos aplicados a los procesos de selección y contratación de trabajadores (anuncio de vacantes, selección y filtro de solicitudes, evaluación de candidatos en las entrevistas/pruebas…), antes de ser comercializados, deberán seguir procedimientos adecuados de evaluación y mitigación de riesgos, tener garantías de alta calidad de los datos empleados que alimentan el sistema para minimizar los riesgos y los resultados discriminatorios[110], tener un registro de la actividad para garantizar la trazabilidad de los resultados, aportar documentación detallada sobre el sistema y su finalidad para que las autoridades evalúen su conformidad, proporcionar información clara y adecuada a los usuarios y contar medidas apropiadas de supervisión humana para minimizar el riesgo. Ahora bien, como ya ha sido apreciado a nivel doctrinal, queda mucho que concretar porque estos requisitos son, en cierto modo, objetivos máximos a los que se debe tender, pero pueden conseguirse de muchas maneras y también con niveles de intensidad diferentes. Se puede aspirar a un nivel máximo, medio o mínimo de calidad o de seguridad[111].

[109] *Vid., infra,* 3.4 y 6.

[110] A estos efectos, el *Libro Blanco sobre IA* establecería que su registro habría de parametrizarse en cuando debe afectar a los datos empleados para entrenar a los sistemas de IA de elevado riesgo y, en algunos casos, la conservación de los datos en sí mismos, para facilitar el seguimiento y la comprobación de las acciones o decisiones de aquellos potencialmente problemáticos, y para que, asimismo, se incentive el respeto de tales normas por los agentes económicos desde el principio. Y, por otra parte, habría de garantizarse la conservación del conjunto de datos utilizado para entrenar y probar los sistemas de IA, especialmente una descripción de sus principales características y el modo en que se escogió el conjunto de datos e incluso, en determinados casos justificados, los propios conjuntos de datos, las metodologías de programación y entrenamiento, así como de validación. Estos requisitos de registro persiguen –así se declara explícitamente- la evitación de sesgos discriminatorios.

[111] Huergo Lora, A., *El proyecto de Reglamento sobre la Inteligencia Artificial,* https://almacendederecho.org/el-proyecto-de-reglamento-sobre-la-inteligencia-artificial, p. 5.

Los Estados miembros deben establecer mecanismos de supervisión y también de sanción[112] y habrán de designar una o varias autoridades nacionales competentes para supervisar su aplicación y ejecución y llevar a cabo tareas de vigilancia del mercado. En términos de gobernanza, la Comisión propone que estas autoridades controlen las nuevas normas, mientras que la creación de un Comité Europeo de IA (con representantes de cada Estado, la Comisión y el Supervisor Europeo de Protección de Datos) facilitará su aplicación e impulsará la creación de normas en materia de IA y generará conocimientos especializados.

Cabría cuestionar si el futuro Reglamento comunitario agotará y resolverá los problemas jurídicos de la IA. Evidentemente no. En el ámbito objeto de este estudio, por ejemplo, al tratarse de aplicaciones de alto riesgo, para los algoritmos empleados en los procesos de selección y contratación de trabajadores, se precisaría mayor concreción y, además, aun cumpliendo con el régimen previsto, ello podría no evitar daños que suponen vulneraciones de derechos (los sistemas *aprenden* en su funcionamiento). Así, el cumplimiento de las obligaciones del Reglamento o de las que puedan fijar las legislaciones nacionales permitiría evitar la sanción (responsabilidad administrativa) pero no así la reclamación por daños y perjuicios (responsabilidad civil) aunque pudiera valorarse en qué medida la responsabilidad queda limitada (¿o excluida?) como consecuencia de la aplicación de esas medidas, que en principio suponen una actuación diligente dirigida a minimizar los riesgos. Es más, en el ámbito del empleo, como veremos a continuación, es necesario valorar las distintas actuaciones y posibles incumplimientos de fabricante (productor, desarrollador) pero también del empresario en el uso de los sistemas de IA.

Aquí, en el específico ámbito de las relaciones laborales (acceso y desarrollo), el poder de dirección tecnológico basado en algoritmos puede derivar en la adopción de decisiones discriminatorias y vulneración de distintas manifestaciones del derecho de privacidad por lo que las garantías han de ir más allá del derecho de transparencia y el control en el diseño de los sistemas de IA. Así, habrá que perfilar una auténtica *gobernanza algorítmica* con implicación de distintos actores[113]: controles públicos (certificación/acreditación –en su caso,

[112] La comercialización y/o uso de sistemas de IA que no cumplan con los requisitos de la Propuesta, habrá de ser sancionada (sanciones efectivas, proporcionadas y disuasorias) y se fijan umbrales en función del tipo de incumplimiento: a) relativo a prácticas prohibidas, 30 millones de euros o el 6% del volumen de negocio anual total a escala mundial del ejercicio financiero anterior, b) incumplimiento de cualquier otro requisito u obligación de la Propuesta, hasta 20 millones de euros o el 4% del volumen de negocio anual y c) suministåro de información incorrecta, incompleta o engañosa a los organismos notificados y/o autoridades nacionales, hasta 10 millones de euros o el 2% del volumen de negocio anual total.

[113] En esta línea, en materia de decisiones automatizadas, ROIG aboga por ir más allá de la responsabilidad algorítmica y avanzar hacia un marco regulador participativo y en constante revisión; una perspectiva dinámica complementaria mediante plataformas formales e informales de cooperación entre la regulación jurídica y las soluciones técnicas: *gobernanza algorítmica* (*Las*

aparato sancionador público, control judicial), privados (auditoría algorítmica, declaración responsable, evaluación de impacto) y participación de sujetos colectivos (derechos de información y consulta, negociación colectiva). Es decir, abarcar actuaciones antes, durante y después de la utilización de algoritmos y contemplar las dimensiones preventiva y reparadora. Tal planteamiento resulta clave en la medida en que, de inicio, de forma consciente o inconsciente podrían haberse incorporado sesgos pero, además, y al margen de aquellos, el algoritmo, se nutre de otras informaciones o comportamientos no representativos de la población que pueden acabar produciendo efectos discriminatorios[114]. Se trataría de aplicar un vigilancia previa y permanente a la IA en las relaciones laborales, no de otra manera proyectaremos la ética al desarrollo tecnológico y haremos confiable la IA.

5. UN INTENTO DE FIJAR INCUMPLIMIENTOS, SUJETOS RESPONSABLES Y SUS CONSECUENCIAS. LAS LÓGICAS PROACTIVA Y REACTIVA

Conforme a lo dicho hasta aquí, el reclutamiento por algoritmo podría concretarse en diversas decisiones, conductas vulneradoras de derechos fundamentales (protección de datos -eventualmente también intimidad y secreto de comunicaciones-, no discriminación). Además, a nivel comunitario se avanzan una serie de garantías que habrán de cumplirse en los procesos de selección de personal a través de algoritmo pues son sistemas de algo riesgo. Así, los eventuales incumplimientos generarían consecuencias indemnizatorias desde la óptica de los derechos fundamentales (uno o varios) y también sancionadoras (protección de datos, empleo) junto con el régimen sancionador que habrá de precisarse tras la futura entrada en vigor del Reglamento sobre IA. Y, en este marco, los posibles sujetos responsables podrían ser el empresario como gestor de las relaciones laborales en la empresa[115] y usuario de sistemas de IA y el fabricante, desarrollador del algoritmo (prestadores, en el lenguaje de la Propuesta de reglamento, «*que introducen en el mercado o ponen en servicio sistema de IA»)*.

El panorama expuesto exige, a todas luces, una labor de adaptación, actualización y también de creación en el ámbito de la responsabilidad, principalmente, administrativa y civil. Algo ya anunciado como necesario –como avanzamos- en la

garantías frente a las decisiones automatizas. Del Reglamento General de Protección de datos a la Gobernanza algorítmica, Ed. Bosch, Barcelona, 2020, p. 20).

[114] CUATRECASAS. Instituto de Estrategia legal en RRHH. Proyecto Technos 2016-2019, *Informe general..., op. cit.,* p. 202.

[115] El empresario, además, podría ser responsable civil por cualquier persona con responsabilidad en materia de selección de personal en la empresa como Departamentos de RRHH o Relaciones laborales o incluso empresas externas de selección contratadas.

Carta de derechos digitales (labor de evaluación y reforma -XXV.4-). Además, como ya referimos también, el diseño de la tutela antidiscriminatoria se enfrenta a nuevos retos en su protección frente a discriminaciones directas e indirectas y se vislumbra ya la necesidad de ampliar aquella a la discriminación algorítmica ante decisiones parciales o finales automatizadas. Aquí, será clave la dimensión proactiva (y sin perder de vista su posible acumulación a la reactiva, pese a las dificultades que, en ocasiones, puede presentar) y la base de esta protección serían -en línea, como vimos, con la visión de la AEPD- la transparencia, la explicabilidad, la evaluación de impacto y la auditoría algorítmica[116]. Sólo a través de la transparencia y explicabilidad podrá evaluarse si el impacto discriminatorio deriva de la (falta de) calidad de los datos, de la forma en que trabajan, o/y de los poderes de predicción algorítmicos[117].

En este contexto, de cierto *impasse* normativo, y en el específico ámbito de la selección y contratación de trabajadores podríamos pensar en varias situaciones posibles:

- El fabricante/desarrollador del sistema de IA cumple con el marco regulador futuro de IA pero aun así se han producido daños. Aquí ya se plantea si, en el marco de la responsabilidad, no sería oportuna la fijación de la obligación para aquel de concertar seguro obligatorio de responsabilidad civil[118].
- El fabricante/desarrollador y el empresario cumplen en origen pero se producen resultados lesivos de derechos fundamentales (*deep learning*). Aquí, centrándonos en el empleador, podríamos cuestionar si aplicar un esquema de responsabilidad objetiva por daño en tanto que garante de la igualdad en las relaciones de trabajo en la empresa, con la posibilidad de valorar la concurrencia de factores que aminoren o excluyan la responsabilidad.
- El fabricante/desarrollador del sistema de IA no cumple, el empleador tampoco. El proveedor informático diseñó el algoritmo con sesgos que arrojan resultados discriminatorios y el empresario lo sabe o incluso lo ordenó (oculta propósitos discriminatorios detrás del algoritmo). Además, no cumple aquel las exigencias (futuras) de los sistemas de IA de algo riesgo.

[116] Sáez Lara aboga por llevar a cabo las reformas normativas necesarias como la oportuna inclusión en el art. 17 ET de la referencia o llamada de atención al uso de aplicaciones de IA con la obligación legal de que el empresario realice la evaluación de impacto discriminatorio de las decisiones automatizadas, incluidas la elaboración de perfiles, con efectos sobre las personas trabajadoras, en el momento de su contratación o durante su relación laboral ("Algoritmo y discriminación en el empleo..., *op. cit.,* ps. 14 y 17).

[117] Sáez Lara, C., "El algoritmo como protagonista de la relación laboral, *op. cit*., p. 58.

[118] CUATRECASAS. Instituto de Estrategia legal en RRHH. Proyecto Technos 2016-2019, *Inteligencia artificial. Impacto en la organización del trabajo...,* p. 44.

 Recepción original: 08.04.2021. Aceptación: 18.04.2021

De partida, el empresario podría ser demandado en proceso de tutela de derechos fundamentales y condenado a pagar indemnización por daños y perjuicios pero también el fabricante pues a tenor del art. 177. 1 LRJS pueden ser legitimados pasivos en este procedimiento los «*terceros vinculados al empresario por cualquier título, cuando la vulneración alegada tenga conexión directa con la prestación de servicios»,* lo que permite incluir, entendemos, los procesos de selección. No obstante, la dificultad probatoria ya presente en todos los supuestos de discriminación en el proceso de acceso a un puesto de trabajo se acrecienta aquí, al tener que constatar de un lado, que el algoritmo es sesgado y, de otro, que el empleador fue responsable de ello[119].

Imaginemos que el algoritmo de selección fue creado con sesgos y, además, se han vulnerado las obligaciones en materia de protección de datos, se producirían, entonces, dos vulneraciones de derechos fundamentales con las correspondientes obligaciones de reparación privadas y también podría entrar en escena el marco sancionador público. En estos casos, el sujeto pasivo es el empresario que es, además, el responsable del tratamiento[120] y podríamos pensar en las sanciones de la LISOS y de la LOPDPyGDD. Conforme al art. 16.1.c) LISOS será infracción administrativa muy grave «*Solicitar de datos de carácter personal en los procesos de selección o establecer condiciones, mediante publicidad, difusión o cualquier otro medio, que constituyan discriminación en el acceso al empleo por motivos de sexo, origen, incluido el racional o étnico, edad, estado civil, discapacidad, religión o convicciones, opinión política, orientación sexual, afiliación sindical, condición social o lengua dentro del Estado»)* mientras que en la norma interna de protección de datos, el catálogo de sanciones administrativas es mucho más amplio (arts. 70-78 LODPyGDD) y alcanza a infracciones leves, graves y muy graves que podrían aplicarse a incumplimientos en materia de protección de datos en los procesos de selección de personal y contratación de trabajadores. Así, por ejemplo, el incumplimiento de las obligaciones del art. 22 RGPD en relación a las decisiones individuales automatizadas sería infracción constitutiva de sanción muy grave si se tratara de impedimento, obstaculización o no atención reiterada al ejercicio de los derechos allí establecidos, conforme a la LOPDPyGDD (art. 72. b)[121] y no

[119] Rivas Vallejo, P., *La aplicación de la inteligencia artificial al trabajo..., op. cit*., p. 343.

[120] La responsabilidad del encargado de tratamiento es, como se conoce, más limitada, pues únicamente responde de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones normativas dirigidas específicamente a los encargados o cuando haya actuado al margen o en contra de instrucciones legales del responsable (art. 82.5 RGPD).

[121] También podría ser infracción leve la no atención a las solicitudes de ejercicio de los derechos establecidos en ese art. 22 RGPD, cuando no sean constitutivas de infracción muy grave (art. 74 d] LOPDPyGDD).

conforme a la LISOS[122]. De cualquier forma, al aparato sancionador descrito habrá que sumar, cuando en los procesos de selección y contratación de trabajadores intervengan algoritmos, las futuras sanciones administrativas por incumplimiento de obligaciones en estos sistemas de alto riesgo.

- El fabricante cumple, el empresario no. Por ejemplo, manipula el sistema o comprueba que el algoritmo está captando datos que no debe y/o es discriminatorio, no se respetan las garantías del art. 22 RGPD... y no adopta medida alguna para evitarlo. Tal actuación se concretaría en responsabilidad civil del empresario por vulneración de derechos fundamentales y responsabilidad administrativa en los términos expuestos.

6. ESPACIOS PARA LA REPRESENTACIÓN DE LOS TRABAJADORES Y LA NEGOCIACIÓN COLECTIVA

Al margen de tecnología, en materia de acceso al empleo, la negociación colectiva incluye controles en el proceso y garantías frente a la no discriminación. Como ejemplo, el XVII Convenio colectivo estatal de empresas de Consultoría y estudios de mercado y de la opinión pública[123] establece que en caso de reclamación contra la selección efectuada formulada por alguna persona trabajadora de la empresa que se estime injustamente pospuesta a favor de otra persona, el Comité de Empresa tendrá acceso a las Actas o Informe de evaluación y demás documentación del proceso selectivo relativas al empleado reclamante y al aspirante seleccionado[124].

El reclutamiento tecnológico y su potencial discriminatorio, supone, sin embargo, un paso más en la necesaria fijación colectiva de controles y garantías por parte de la representación de los trabajadores y la negociación colectiva.

[122] Lógicamente, las posibles sanciones administrativas no serían acumulables si recayeran en los mismos sujetos, en base a los mismos hechos y fundamentos jurídicos (*non bis in ídem*) y, en tal caso, impuesta una sanción por una de las autoridades (AEPD, Autoridad laboral) la otra autoridad habría de cesar en su actuación. En definitiva, operaría una especie de regla implícita de prioridad en la actuación temporal, la primera que resuelve bloquearía la continuidad de la segunda (Cruz Villalón, J., *Protección de datos personales del trabajador..., op. cit.,* p. 91).

[123] Resolución DGE de 22 de febrero de 2018 (https://www.boe.es/boe/dias/2018/03/06/pdfs/BOE-A-2018-3156.pdf).

[124] Los procesos de selección asegurarán, además, la objetividad y no discriminación de la misma y en ellos tendrán preferencia para ocupar el puesto o puestos de trabajo que se pretendan cubrir con el nuevo o nuevos contratos, el personal de la empresa, siempre que obtenga igual evaluación en el proceso selectivo que las personas aspirantes a ingresar en la plantilla. La empresa informará por escrito al inicio del proceso de selección a los representantes de los trabajadores del tipo de proceso, filtros y actividades relacionadas con la selección (art. 12).

Ello nos conduce a la idónea articulación a este nivel del necesario derecho de transparencia. Esto es, derecho de información individual y colectiva, información que ha de ser básica y asequible (no hay que llegar al código fuente).

En este contexto, el *Acuerdo Marco Europeo de los interlocutores sociales sobre digitalización*[125] (2020) recoge, entre sus principios básicos, la garantía del principio de control humano en la IA. Ello se concreta en que el despliegue de estos sistemas debe seguir aquel principio, deben ser seguros y evitar riesgos (evaluación de riesgos e inclusión de oportunidades para mejorar la seguridad y prevenir riesgos), seguir principios de equidad asegurando que los trabajadores y grupos estén exentos de prejuicios y discriminación injustos y ser transparente y explicable con una supervisión efectiva (su grado dependerá del contexto, gravedad y consecuencias)[126]. Así, los convenios colectivos y acuerdos de empresa habrían de incorporar previsiones específicas en esta línea en materia de ingreso cuando la empresa utilice IA en los procesos de selección de personal. O, al menos, consultar e informar a los representantes de los trabajadores su introducción y utilización. La Comunicación de la Comisión *Generar confianza en la inteligencia artificial centrada en el ser humano*[127] apunta tal necesidad cuando la implementación de sistemas de IA en la empresa pueda provocar cambios en la organización del trabajo, la vigilancia y su control, así como en los sistemas de evaluación y contratación de trabajadores.

La Ley de Secretos empresariales de 2019 ya habría avanzado la posibilidad de obtener de manera lícita secretos empresariales cuando sean cuestiones relacionadas con el ejercicio de los derechos de los trabajadores y los de representación de estos (art. 1.3). Trasladado a la IA, ello no puede entenderse en el sentido de que haya de revelarse todo el algoritmo sino sus bases o lógica de funcionamiento[128]. Ahora, en esta línea ya, como se refirió previamente, el apartado dos del artículo único del RD Ley 9/2021 incorpora, una nueva letra d) en el art. 64.4 ET que establece el derecho de los representantes de los trabajadores de ser informados por la empresa de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de IA que afecten a la toma de decisiones que pueden incidir en las condiciones de trabajo, el acceso y el mantenimiento del empleo, incluida la elaboración de

[125] https://www.ccoo.es/3ec9e3ddff84034c1a796cb52ac84c09000001.pdf

[126] *Vid*., Baz Rodríguez, J., "El Acuerdo Marco Europeo sobre digitalización: un instrumento esencial para el desarrollo de los derechos digitales laborales en Europa", en AA.VV. (dir. J. Baz Rodríguez), *Los nuevos derechos digitales laborales de las personas trabajadoras en España. Vigilancia tecnificada, teletrabajo, inteligencia artificial*, Ed. Wolters Kluwer, Madrid, 2021, ps 436 y ss.

[127] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2019:168:FIN

[128] Creix, J., *Los algoritmos que rigen las relaciones laborales: así son y así se regulan.* https://cincodias.elpais.com/cincodias/2021/05/13/companias/1620936778_868244.html, 13 mayo 2021.

perfiles. Se recoge, por tanto, un derecho de información pasiva que se avanzaría, como vimos, en la *Carta de derechos digitales*[129].

Una precisión adicional, la protección frente a los secretos empresariales se dispensa a su titular que es «*cualquier persona física o jurídica que legítimamente ejerza el control sobre el mismo*» y se extiende frente a cualquier modalidad de obtención, utilización o revelación de información. Será el empresario el protegido por la ley cuando sea él el que ha diseñado, desarrollado el algoritmo de selección de personal pero, si no ha sido así (lo más frecuente), sino que lo ha hecho un proveedor tecnológico, es necesario incorporar algunos matices. De un lado, podrían surgir responsabilidades (acciones civiles por daños y perjuicios) del empresario frente al proveedor tecnológico si este revelara datos esenciales de algoritmo (más allá de la transparencia suficiente y de la lógica de funcionamiento del mismo) y, de otro, el empresario solo podrá cumplir con su obligación de transparencia frente al algoritmo (frente a los representantes de los trabajadores o acciones individuales en caso de vulneración del derecho de protección de datos o indicios de discriminación) cuando se le haya aportado esa información. De ahí la importancia de cumplimiento y articulación de la obligación que establece la Propuesta de Reglamento sobre la información adecuada y suficiente a los usuarios en los sistemas de IA de alto riesgo.

Siguiendo con la negociación colectiva, el XXIX Convenio colectivo del sector de la banca 2021[130] ya incorpora previsiones en este sentido centradas en las decisiones automatizadas y el derecho de información y trasparencia frente al algoritmo. El art. 80.5, bajo la rúbrica *Derechos ante la IA* comienza afirmando que las nuevas herramientas basadas en algoritmos pueden aportar valor hacia una gestión más eficiente de las empresas, ofreciendo mejoras en sus sistemas de gestión. Sin embargo, el desarrollo creciente de la aportación de la tecnología requiere de una implantación cuidadosa cuando se aplica en el ámbito de las personas. Por ello, las personas trabajadoras tienen derecho a no ser objeto de decisiones basadas única y exclusivamente en variables automatizadas, salvo en aquellos supuestos previstos por la Ley, así como derecho a la no discriminación

[129] *Vid. supra,* 2.

[130] Resolución de 17 de marzo de 2021 que registra y publica el XXIV Convenio colectivo del sector de la banca (BOE 30 marzo 2021).

Otro ejemplo previo de contenido más limitado, el anexo del II Convenio colectivo de puertos de Estado y autoridades portuarias (prorrogado provisionalmente en el III Convenio colectivo -2019-2026 –BOE 13.6.2019 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-9021-) establecería que Recursos Humanos seleccionaría a los empleados, en número igual al requerido, mediante la aplicación del algoritmo de distancias con respecto al perfil necesario. En caso de existir más empleados de los necesarios con distancia idéntica, se realizarían las pruebas de selección complementarias. En materia de garantías se recogería que los perfiles personales de todos los trabajadores y las herramientas de medida (algoritmo de distancia) están a disposición de los miembros de la Comisión Local.

en relación con las decisiones y procesos cuando ambos estén basados únicamente en algoritmos, pudiendo solicitar, en estos supuestos, el concurso e intervención de las personas designadas a tal efecto por la empresa en caso de discrepancia.

Además, las empresas informarán a la representación legal de los trabajadores sobre el uso de la analítica de datos o los sistemas de IA cuando los procesos de decisiones en materia de recursos humanos y relaciones laborales se basen exclusivamente en modelos digitales sin intervención humana. Dicha información abarcará, como mínimo, los datos que nutren los algoritmos, la lógica de funcionamiento y la evaluación de resultados. La concreción en este convenio colectivo del derecho de transparencia frente al algoritmo reproduce, exactamente, los derechos digitales en el ámbito laboral de la *Carta de derechos digitales* (XVII.4).

El referido derecho de información de los representantes de los trabajadores del art. 64.4.d) ET supone un primer paso en la articulación del derecho de transparencia frente al algoritmo y en esa dimensión colectiva de protección frente a la IA (gobernanza colectiva)[131]. En la misma línea, esa referencia negocial del convenio de Banca va un poco más allá (como mínimo, datos, lógica y evaluación de resultados frente a los parámetros, reglas e instrucciones en los que se basan los algoritmos de la ley). Además, no se admiten decisiones totalmente automatizadas –salvo excepciones- siendo requerida intervención humana, se recuerda el derecho a la no discriminación en relación con las decisiones y procesos basados (únicamente) en algoritmos y se establece un mecanismo de solución intraempresarial en caso de conflicto (con intervención de las personas designadas por la empresa).

Puede ser un buen comienzo pero, sin duda, la presencia creciente de la IA en la gestión de las relaciones de trabajo en las empresas y su potencial hacia el futuro, exigirá intensificar los controles colectivos que han de venir de la negociación colectiva y de las competencias de los representantes de los trabajadores. No olvidemos que las obligaciones que la Propuesta de reglamento establece para los sistemas de algo riesgo son objetivos que admiten distintos grados de concreción y realización y aquí la acción colectiva será clave. Por ello, en aquellos aplicados a los procesos de selección y contratación de trabajadores, que antes de ser comercializados, deberán seguir procedimientos adecuados de evaluación y mitigación de riesgos, los representantes de los trabajadores podrían requerir auditoría de IA. Esto es, que el modelo algorítmico ha pasado el control correspondiente a efectos de filtración de sesgos discriminatorios en su uso y, en su aplicación, las oportunas revisiones periódicas para testar con la periodicidad

[131] Sobre esta idea, desde los datos personales, Todolí, Signes, A., "La gobernanza colectiva de la protección de datos en las relaciones laborales: Big Data, creación de perfiles, decisiones empresariales automatizadas y derechos colectivos", RDS, nº 84, 2018 y Mantelero, A., "Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection", *Computer Law &Security Review,* nº 32, 2016, ps. 238 y ss.

necesaria la regularidad de su funcionamiento[132]. Además, -y siguiendo en el marco de las obligaciones que, de momento, fija la Propuesta comunitaria deberían contar con la información relativa a las garantías de alta calidad de los datos empleados que alimentan el sistema para minimizar los riesgos y los resultados discriminatorios y tener acceso al registro de la actividad para garantizar la trazabilidad de los resultados y a la documentación detallada sobre el sistema y su finalidad que habría aportar el proveedor a la empresa. También habrían de tener competencias para verificar, de un lado, que la información aportada a los usuarios es clara y adecuada y, de otro, que las medidas de supervisión humana para minimizar el riesgo, son apropiadas.

El espacio colectivo de la IA en la empresa es grande y es un nuevo desafío en la acción de representación y defensa de los intereses de los trabajadores. En este sentido, además, en el específico campo de la no discriminación en el acceso al empleo y partiendo de esa idea de la ambivalencia del algoritmo en este campo, ya se plantea, la oportunidad de admitir que los propios sindicatos hagan uso de herramientas algorítmicas para la medición de patrones de discriminación. Como expone Rivas Vallejo, al ser posible el diseño de modelos algorítmicos para detección de patrones históricos, sería posible su aplicación a la búsqueda del sesgo en las decisiones empresariales y aquí se conformaría como herramienta procesal para la tutela de derechos fundamentales en el plano probatorio. Bastaría alimentar al algoritmo con datos históricos relativos al hipotético empresario autor de la vulneración[133].

Todo lo expuesto exigirá, sin duda, un esfuerzo de capacitación y actualización permanente por parte de los sujetos colectivos. No de otro modo podrá llevarse a buen término ese control al poder de dirección tecnológico.

[132] La auditoría de algoritmos es una herramienta propuesta por la ingeniería informática como método adecuado de control de sesgos en la utilización de la IA (Véase, EURECAT [*http://eurecat.org/es/ambitos-de-conocimiento/big-data/*], Rivas Vallejo, P., *La aplicación de la inteligencia artificial..., op. cit.,* p. 284).

[133] *La aplicación de la inteligencia artificial al trabajo, op. cit.*, p. 361.