

FICHAS CIENTÍFICO-TÉCNICAS

NUEVAS TÉCNICAS DE REGULACIÓN-GESTIÓN SOCIOLABORAL JUSTA EN LA ERA DIGITAL

2 | PRINCIPIO DE PRECAUCIÓN: ¿MEJORAS DE EFICIENCIA O RIESGO DE DISCRIMINACIÓN?

Cristóbal Molina Navarrete
*Catedrático de Derecho del Trabajo y
de la Seguridad Social. Universidad de Jaén*

TRANSFORMA 
e-work 

Transformaciones del trabajo en la economía digital:
Condiciones económicas y sociales para una transición justa
RTI2018-099337-B-C21

1. No todo son ventajas en la gestión laboral Big Data: la práctica reafirma la necesidad de regulación según un enfoque de gestión de riesgos para los derechos

1 Para conocer las pautas en torno al tratamiento automático e individualizado del Comité Europeo de Protección de Datos (antiguo GT 29), vid. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. https://ec.europa.eu/news-room/article29/item-detail.cfm?item_id=612053

2 <https://rm.coe.int/msi-aut-first-meeting-report-6-7-march-2018/16807971b5>

3 Vid. MUÑOZ RUIZ, A.B. ¿Se deben regular los algoritmos? Un breve análisis a la propuesta normativa alemana: la pirámide de criticidad basada en el riesgo. <https://forodelabos.blogspot.com/2019/12/se-deben-regular-los-algoritmos-un.html>

4 <https://www.expansion.com/economia-digital/companias/2020/02/19/5e4d7b67e5fdeabc348b45ad.html>

1.1. Exigencia normativa del enfoque de evaluación de riesgos individuales (EIPD) para el tratamiento Big Data

Hasta aquí hemos visto la parte positiva de los usos Big Data en el ámbito socio-laboral y en consecuencia las razones e intereses que favorecen su desarrollo. Ahora bien, contiene también una parte “negativa”, como “fuente de (nuevos y emergentes) riesgos”. Este enfoque de gestión de riesgos está en el Reglamento 2016/679/UE, del Parlamento y del Consejo, Reglamento General de Protección de Datos (RGPD), concretamente sus arts. 22 y 35.3.

El primero, prohibiría, con carácter general, la adopción de decisiones —privadas y públicas— individuales exclusivamente automatizadas, incluida la elaboración de perfiles¹, salvo que cuente con un título legítimo, conforme a su apartado 2. En los casos de tratamiento automatizado por necesidades del contrato —aquí de trabajo, en nuestro caso—, o cuando medie consentimiento —menos eficaz en el ámbito de las relaciones de trabajo—, requiere del responsable del tratamiento que adopte “las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, **como mínimo el derecho a obtener intervención humana** por parte del responsable, a expresar su punto de vista y a impugnar la decisión” (ejemplo, de evaluación de rendimiento, o de despido; o de no selección para el empleo). Se trataría del derecho fundamental a obtener una justificación humana de la decisión, sin que se base solo en la IA o en decisión algorítmica.

En virtud del segundo precepto comunitario, es obligatoria la “**Evaluación de Impacto relativa a la protección de datos**” (EIPD) cuando medien procesamientos masivos. Entre los aspectos que ha de incluir están, junto a la actividad a desarrollar y la proporcionalidad de los medios en relación a los fines perseguidos, tanto (1) **la evaluación de los riesgos para los derechos y libertades** de los interesados (no sólo su derecho a la intimidad, a la imagen o libertades de expresión, también el derecho a la no discriminación) cuanto (2) **las medidas** previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos **que garanticen la protección de datos personales**.

Más recientemente, esta necesidad de regulación de la ITA y los tratamientos Big Data con un enfoque de gestión de riesgos es reconocida por la *Comisión Ética de Datos* constituida por el Gobierno alemán. Su propuesta se enmarca en el debate sea en torno a la necesidad de una regulación específica, que vaya más allá del RGPD, si bien no queda claro sí en el plano nacional (*The Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence, MSI-AUT 2018*²), o comunitario, sea sobre el papel de la autorregulación. **La posición alemana parece favorecer una regulación comunitaria, pero flexible**³.

Cómo no, la Comisión ha recogido ese guante y propone una regulación específica de los sistemas de gestión basados en la Inteligencia Artificial (IA)⁴. En la Figura 1 de esta Ficha se dejaron claras las relaciones entre los sistemas de tratamiento de datos Big Data y los propios de la IA y Algoritmos (la IA y los Algoritmos permiten convertir en conocimiento para adoptar una decisión la ingente información proporcionada por el sistema Big Data). La Unión Europea impulsa un modelo de regulación ético-confiable del desarrollo de la IA y de los procesos de decisión por algoritmos para garantizar que se respetan los derechos fundamentales, sobre la base de considerarlos “sistemas de tratamiento de alto riesgo a certificar, probar y controlar”. Con ello no sólo se pretende proteger la privacidad sino también la prohibición de gestión por sesgos discriminatorios, así como corregir la falta de transparencia decisional.

1.2. No, tampoco es pura especulación: Reafirmación de la necesidad de reglas basadas en el enfoque de riesgos a través de las experiencias (negativas)

La experiencia más reciente alerta de la inherencia de altos riesgos a los sistemas avanzados de gestión digital (Big Data, IA, Algoritmos). La proliferación de usos peligrosos, sesgados y opacos de tales sistemas está a la orden del día. AMAZON es una fuente inagotable de tales experiencias de riesgos, de ahí que la propia empresa sigue, de momento de manera libre, un método de “ensayo-error”. Así, primero

2

PRINCIPIO DE PRECAUCIÓN: ¿MEJORAS DE EFICIENCIA O RIESGO DE DISCRIMINACIÓN?

FICHAS CIENTÍFICO-TÉCNICAS

NUEVAS TÉCNICAS DE REGULACIÓN-GESTIÓN SOCIOLABORAL JUSTA EN LA ERA DIGITAL



tuvo que reconocer los sesgos de género del algoritmo diseñado para el reclutamiento y la promoción profesional, descartándolo una vez se dio cuenta de que discriminaba a las mujeres para puestos técnicos⁵. Luego tuvo que salir al paso de las informaciones que, como se evidenció, la acusaban de despedir a las personas tan sólo por la decisión automática de un algoritmo de evaluación del rendimiento, señalando que no sólo tal procedimiento estaba extendido en las empresas tecnológicas, sino que, además, establecía avisos previos de alerta de reducción progresiva, de modo que no se trataría de un despido automático “expres”. Sin embargo, lo que no ha podido clarificar es en qué criterios de definición y supervisión se basa el referido algoritmo, manteniéndose opacos.

Las noticias de este tipo están a la orden del día en todos los países. Así, en Italia, se denuncia sindicalmente: “Frank, l’algoritmo che discrimina”. El sindicato GGIL ha presentado una demanda contra un algoritmo, llamado “Frank”, utilizado por una empresa multinacional de entrega de alimentos (empresas de economía mediante plataformas digitales) para la distribución de los pedidos. Para el sindicato, marginaría a los trabajadores que, por razones relacionadas con el ejercicio de derechos como la protección frente a la enfermedad y la huelga, no tienen una plena disponibilidad⁶.

Y si de la empresa nos trasladamos a los Servicios Públicos de Empleo, la situación sería análoga. Es el caso, por ejemplo, del célebre programa experimental de la Agencia de Empleo austriaca. Desde hace varios años vendría evaluando la empleabilidad de las personas candidatas a desempeñar un empleo (tasa de oportunidad de hallar un empleo) a través de un sistema algorítmico. No habría mayor problema al respecto, pues hay interés legítimo (mejorar la empleabilidad de las personas desempleadas, lo que es un derecho constitucional), si no fuese porque se han detectado sesgos discriminatorios en sus criterios de puntuación.

En este sistema, no hay un tratamiento exclusivamente automatizado, pues el servicio siempre puede corregir el juicio algorítmico (art. 22 RGPD). Ahora bien, el hecho es que los colectivos de personas con más vulnerabilidad ocupacional resultan perjudicados, ocupando el grupo con puntuaciones clara-

mente peyorativas. Es más probable que el algoritmo AMS asigne a una mujer desempleada a un grupo inferior aun con experiencia y calificaciones coinciden con las de un hombre. El servicio de empleo austriaco (Agencia AMS) no ve problema, sobre la base del carácter neutral propio de una decisión algorítmica, propiciando grandes “ganancias de eficiencia en la gestión”⁷. El problema es que un servicio público de empleo debe respetar de forma efectiva los derechos fundamentales de las personas, así como dar transparencia a sus criterios de gestión. Así lo ha entendido, recientemente, un tribunal holandés, que ha anulado un sistema indicador de riesgo llamado “SyRI” (acrónimo de “System Risk Indication”), por violar la privacidad ex art. 8 CEDH y a la no discriminación. Lo utilizaba el Ministerio de Asuntos Sociales y de Empleo **para rastrear posibles fraudes sociales** (pensiones, subsidios)⁸.

El sistema se basa en la atribución de una tasa de riesgo, a través de computación por un algoritmo preventivo, a cada beneficiario atendiendo a la probabilidad de defraudar. El Tribunal de Distrito de La Haya tuvo en cuenta el informe emitido por el relator especial de la ONU sobre pobreza y derechos humanos, que señalaba sesgos discriminatorios (perjudicaba a las personas ciudadanas con menos renta). En cambio, no tuvo en cuenta la alegación técnica del Ministerio, según el cual, el sistema solo asociaba datos que el Estado (cada vez más digital) ya poseía, dibujando con ellos un árbol de decisión [un modelo de predicción], de modo que no se usa la inteligencia artificial ni algoritmos de autoaprendizaje. Como se ve, una línea argumental análoga a la austriaca. Pero para el Tribunal, tal afirmación “no se puede comprobar, porque la legislación que permite el uso de SyRI no es lo bastante transparente”. Por lo tanto, el Estado mantendría en la oscuridad —“secreto”— la forma de calcular la posibilidad de fraude, lo que iría en contra de los principios que vertebran los sistemas de Bienestar y los Estados de Derecho⁹.

5 <https://www.expansion.com/economia-digital/innovacion/2020/03/01/5e56abf0468aeb681a8b45fd.html>

6 <https://www.rassegna.it/articoli/si-chiama-frank-lalgoritmo-che-discrimina>

7 La noticia está disponible en “Austria’s employment agency rolls out discriminatory algorithm, sees no problem”. <https://algorithmwatch.org/en/story/austrias-employment-agency-ams-rolls-out-discriminatory-algorithm/>

8 La noticia se desglosa con pormenores en “Países Bajos veta un algoritmo acusado de estigmatizar a los más desfavorecidos”. https://elpais.com/tecnologia/2020/02/12/actualidad/1581512850_757564.html

9 Para la metáfora de los Estados de Bienestar digitales como “caballos de Troya de hostilidad neoliberal hacia la protección social y la regulación”. Vid. “Países Bajos veta un algoritmo acusado de estigmatizar a los más desfavorecidos”. https://elpais.com/tecnologia/2020/02/12/actualidad/1581512850_757564.html?ssm=FB_CC&fbclid=IwAR-0vhX8tvGMB9ebR4cwbkkRj00UQep-fSCYsxtvkvfSpDE4q5Mni_JzPhlyjs

2

PRINCIPIO DE PRECAUCIÓN: ¿MEJORAS DE EFICIENCIA O RIESGO DE DISCRIMINACIÓN?

FICHAS CIENTÍFICO-TÉCNICAS

NUEVAS TÉCNICAS DE REGULACIÓN-GESTIÓN SOCIOLABORAL JUSTA EN LA ERA DIGITAL



2. Limitaciones del Derecho actual y vías de progreso: El principio de precaución y el enfoque de gestión de riesgo en los sistemas Big Data

¹⁰ Vid. GARCIA COCA, O. La protección de datos de carácter personal en los procesos de búsqueda de empleo, Laborum, Murcia, 2016.

¹¹ <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3A132042>

2
PRINCIPIO DE PRECAUCIÓN:
¿MEJORAS DE EFICIENCIA O RIESGO DE DISCRIMINACIÓN?

FICHAS CIENTÍFICO-TÉCNICAS

NUEVAS TÉCNICAS DE REGULACIÓN-GESTIÓN SOCIOLABORAL JUSTA EN LA ERA DIGITAL

2.1. ¿Por qué un enfoque de precaución en la gestión laboral Big Data?: Usos implícitos

En definitiva, el plus de riesgo para el respeto de los derechos fundamentales ligados al tratamiento masivo de datos, y en especial para el derecho a la no discriminación es ahora ya una realidad acreditada. Desde esta perspectiva experimental gana razón de ser la propuesta ya citada de una regulación normativa de estos sistemas de Big Data-Inteligencia Artificial sobre la base de un enfoque de riesgo, como apunta el RGPD y profundiza la Comisión alemana de ética de los datos y por la propia Comisión Europea.

Evidentemente, la regulación deberá atender, así como la gestión en cada caso, a las variables de probabilidad y severidad del daño para derechos e intereses de las personas a raíz del recurso a los tratamientos automatizados de datos y a las decisiones de algorítmicas. Como para el sistema de gestión preventiva de riesgos laborales, a mayores sean los niveles de riesgo para los derechos mayores serán las obligaciones de protección eficaz, incluso de una forma anticipada, previa a la actualización del daño, claro está. Surge la cuestión de establecer los diferentes niveles de riesgo para los derechos de las personas en las relaciones de empleo, de trabajo y de protección social, que son las aquí analizadas y, en coherencia, fijar las “medidas adecuadas” de protección.

Ahora bien, ¿cuáles son esas medidas adecuadas cuando la propia Comisión reconoce que son inherentes altos niveles de riesgo a la IA sin que, al tiempo, estemos en condiciones hoy de conocer con certeza hasta dónde llegan de verdad las posibilidades de control humano del funcionamiento del algoritmo, incluso dadas las limitada transparencia en un buen número de casos, como destaca el tribunal holandés? ¿Será en estos casos suficiente con aplicar, aun de forma extensiva, las garantías anti-discriminatorios más evolucionadas (leyes prohibitivas de determinados usos, como sucedería respecto de los datos extraídos de redes sociales para la selección de personal, en EEUU o en Alemania¹⁰), así como el enfoque de transparencia y de evaluación preventiva de riesgos del art. 35 RGPD? ¿No sería conveniente una medida más incisiva,

ya desde el diseño del tratamiento, en línea con lo que requiere el art. 25 RGPD?

Justamente, cuando de la protección efectiva de derechos fundamentales se trata en un doble escenario típico tanto de (1) **análisis, gestión y comunicación de riesgos** relevantes para derechos de las personas cuanto de (2) notable **incertidumbre científica** sobre su impacto negativo concreto en ellos, estamos en el terreno propio del “**principio de precaución**”. Cierto, sus ámbitos originarios y más propicios son el derecho a la protección del ambiente de calidad y el derecho a la protección de la salud (humana, animal o vegetal), hoy tan “a flor de piel” (por la doble emergencia climática y de epidemia por el coronavirus —paradójicamente, esta segunda juega a favor de la corrección parcial de la primera—). Pero, como la Comisión Europea ha evidenciado, esta originaria conformación no impediría su proyección más allá de ambos escenarios típicos [Comunicación de 2 de febrero de 2000, sobre el recurso al principio de precaución¹¹]. En particular, siempre que los datos científicos no permitan una determinación completa del riesgo (en nuestro caso para la privacidad, o, sobre todo, para la no discriminación, incluso para la salud de las personas trabajadoras, en determinados casos, etc.), el recurso a este principio permite adoptar determinadas medidas incisivas de protección, como el proceder a la prohibición de su uso (como ha hecho, aun sin invocar este principio, el tribunal holandés), o mayores garantías de transparencia, colectiva e institucional, etc.. La Comisión considera que este **principio de precaución** es útil para fijar un nivel de protección “adecuado” a la magnitud del riesgo a pesar de la falta de total certeza sobre sus efectos —a diferencia de lo que sucede con el **principio de prevención**, que implica el deber de prevenir todo aquél factor de riesgo que científicamente esté suficientemente acreditado, conforme a la evolución de la ciencia y la tecnología—, permitiendo reacciones más tempranas y eficaces.

A nuestro juicio, también sin mencionarlo expresamente, el Tribunal de la Haya ha hecho un uso implícito del principio de precaución para anular el sistema de gestión analítico-predictiva de conductas de fraude social del Gobierno holandés. El presupuesto defendido por el órgano judicial es la de



tratarse de un “perfil de riesgo creado” a partir de la información de ciudadanos que han delinquido, por lo que “podría estar incurriendo en una discriminación”. Ahora bien, como no hay certeza jurídica de que así sea, traslada la “carga de la prueba” de que no hay riesgo real de discriminación al sujeto responsable de ese tratamiento. Aceptando la legitimidad inicial de la lucha antifraude social (art. 6 RGPD), en línea con el uso que de la Big Data y la “minería de datos” hacen muchas empresas privadas (tarjetas de crédito, seguros, etc.), y asumiendo que no hay certeza sobre la producción de discriminación real, el tribunal concluye que no puede legitimar un “modelo de riesgo” que, en el estado actual de desarrollo del SyRI, “pudiera tener un efecto no sólo estigmatizador sino discriminatorio de la ciudadanía, por la ingente cantidad de información que recoge”. De este modo, los beneficiarios devienen potenciales sospechosos de fraude, lo que quebraría un principio de confianza esencial en los Estados de Bienestar. En consecuencia, pese a la “ceguera” predicada por los diseñadores de los algoritmos, la realidad manifiesta que reflejan sesgos sociales y discriminaciones, no solo los que pueden tener sus diseñadores, sino también los que pueblan la realidad.

2.2. ¿Qué es el principio de precaución y cuándo utilizarlo?: utilidad en entornos de riesgo sospechado, pero no absolutamente cierto.

El principio de precaución sólo se menciona nominalmente una vez (en el artículo 191 del Tratado de Funcionamiento de la Unión Europea —TFUE—) y pretende garantizar un elevado nivel de protección del medio ambiente mediante tomas de decisión preventivas en caso de riesgo probable, aun no completamente cierto según el estado actual de la ciencia. Como se apuntaba, las limitaciones de su ámbito de origen y de mayor proyección (medio ambiente, alimentación, salud) no ha impedido que se expanda a otros, más o menos conexos, como la política de protección de consumidores y usuarios. El principio de precaución resultaría útil en todo ámbito basado en evaluaciones científicas de riesgos preliminares a la implantación, o al desarrollo, de

una medida, respecto de la cual se tienen elementos razonables para temer que los efectos potencialmente nocivos para un derecho fundamental puedan ser incompatibles con el alto nivel de protección elegido. Para la Comisión, ni la falta de previsión normativa es un factor de inseguridad significativa para su aplicación (STJCE 5 de mayo de 1998, asuntos C-157/96 y C-180/96), ni el —arduo— debate sobre cuándo y cómo utilizar el principio de precaución impide un punto óptimo de equilibrio entre la libertad y los derechos de personas y empresas, de un lado, y la necesidad de reducir el riesgo para los derechos fundamentales de las personas, en ausencia de aquella certeza sobre el riesgo concreto, de otro.

Eso sí, su introducción específica, a través de ese punto de equilibrio correcto, facilita la adopción de las medidas proporcionadas, no discriminatorias, transparentes y coherentes, siempre sobre un proceso de toma de decisiones institucionales bien informado científicamente y objetivamente, aunque no haya certeza plena. La Comisión alerta sobre los peligros de sus usos excesivos, pues sería no sólo una suerte de forma encubierta de proteccionismo sino una barrera al progreso. Al contrario, su infravaloración puede tener altos costes. Por tanto, la Comisión Europea subraya que el principio de precaución solo se puede invocar en situaciones de un riesgo potencial, y que en ningún caso puede justificar una toma de decisión arbitraria.

En suma el recurso al principio de precaución se inscribe siempre en un marco general del análisis de riesgo (evaluación, gestión y la comunicación del riesgo) como presupuesto para la toma de decisiones. Estos procedimientos de toma de decisión deben ser transparentes y participados por todas las partes interesadas y lo antes posible y en la medida en que sea razonablemente viable (gobernanza colectiva). Para la Comisión, el recurso al principio está justificado si se cumplen las tres condiciones siguientes:

- Identificación de los efectos potencialmente negativos del riesgo analizado.
- Evaluación de los datos científicos disponibles.
- Ampliación de la incertidumbre científica.

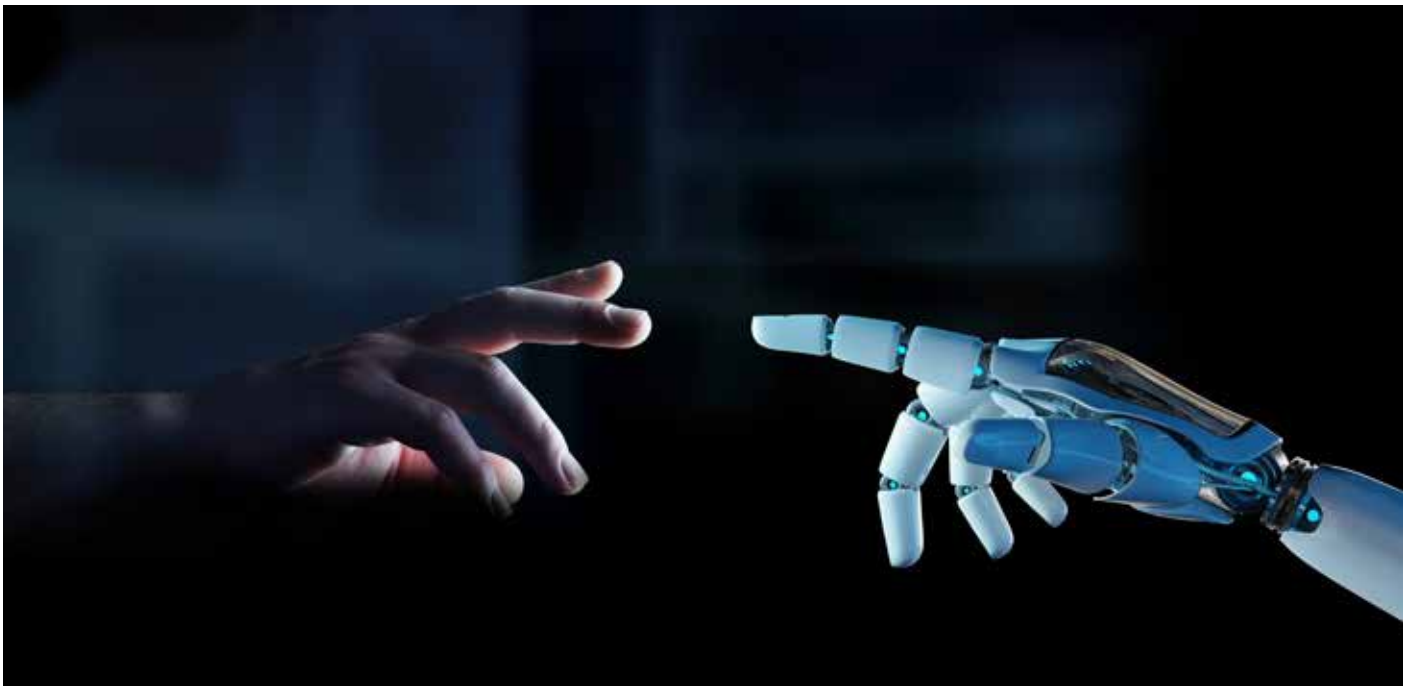
2

PRINCIPIO DE PRECAUCIÓN: ¿MEJORAS DE EFICIENCIA O RIESGO DE DISCRIMINACIÓN?

FICHAS CIENTÍFICO-TÉCNICAS

NUEVAS TÉCNICAS DE REGULACIÓN-GESTIÓN SOCIOLABORAL JUSTA EN LA ERA DIGITAL





¹² Vid. GONZÁLEZ COBALEDA, E. "La digitalización de la economía: ¿cómo desafía la IA a la prevención de riesgos laborales?". <https://www.transformaw.com/blog/los-retos-de-la-digitalizacion-de-la-economia-en-la-prevencion-de-riesgos-laborales/>

¹³ Vid. MUÑOR RUIZ, A.B. ¿Se deben regular los algoritmos? <https://forodelabos.blogspot.com/2019/12/se-deben-regular-los-algoritmos-un.html>

2.3. ¿Qué implica el "principio de precaución" para una regulación más transparente y segura de la IA y Big Data en el ámbito laboral?

No es la primera vez que hacemos un llamamiento a la utilidad, en el actual entorno de innovación tecnológica, al principio de precaución, especialmente en relación a una protección más efectiva de la seguridad y salud en el trabajo. Ya se expuso al analizar la STSJ Navarra 30/2018, 8 de febrero. Esta no considera un obstáculo, para prohibir una contratación laboral, las dudas científicas en torno a cuáles serán los efectos nocivos para la salud de determinadas personas de nuevos materiales (nanopartículas), pues la sola posibilidad razonable, según ciertos informes científicos, de tenerlos legitimaría la prohibición de contratar, por más que

eso cause un perjuicio grave profesional a la persona, que no es compensable, hoy¹².

Vemos, pues, cómo los tribunales hacen uso del enfoque de riesgos típico del principio de precaución, aunque no lo mencionen expresamente. El recurso a este principio supone que se han identificado los efectos potencialmente peligrosos derivados de un producto o un proceso, y que la evaluación científica no permite determinar el riesgo con la certeza total. Precisamente, como se deriva de la propuesta de la *Comisión alemana de Ética de Datos* para la regulación de los algoritmos, si bien tampoco lo alude expresamente¹³, el principio de precaución requiere una evaluación sobre los niveles de riesgo «aceptables-inaceptables». El principio de **precaución implica más un modo concreto de actuar del sujeto de tratamiento automatizado de datos** que un tipo de medida específica. Así:

- En unos casos, puede requerir medidas no obligatorias (autorregulación responsable, recomendaciones, etc.), y, en otros, **demandar una acción vinculante**, con una gama amplia (ej. prohibiciones, compromisos de investigación e información, medidas técnicas u organizativas, deberes de transparencia, etc.).
- Exige la máxima participación de los sujetos implicados, lo que para el ámbito de la IA y el Big Data representa añadir garantías colectivas a las individuales (**gobernanza colectiva del tratamiento automatizado de datos masivo** en el ámbito laboral).
- Inversión de la carga de la prueba:** asignar al sujeto de tratamiento Big Data aportar la evaluación que evidencie que no hay riesgo real de discriminación.

2

PRINCIPIO DE PRECAUCIÓN: ¿MEJORAS DE EFICIENCIA O RIESGO DE DISCRIMINACIÓN?

FICHAS CIENTÍFICO-TÉCNICAS

NUEVAS TÉCNICAS DE REGULACIÓN-GESTIÓN SOCIOLABORAL JUSTA EN LA ERA DIGITAL

