45.ª Sesión Cerrada de la Asamblea Global de Privacidad

octubre de 2023

Resolución sobre Inteligencia Artificial y Empleo

Esta Resolución es presentada por los patrocinadores en nombre del Grupo de Trabajo sobre Ética y Protección de Datos en la Inteligencia Artificial.

PATROCINADORES:

- Information Commissioner's Office (ICO), Reino Unido
- Comisionado Federal de Protección de Datos y Libertad de Información (BfDI), Alemania
- Autoridad de Protección de Datos (Garante per la protezione dei Dati Personali - GPDP), Italia

COPATROCINADORES:

- Comisionado Federal de Protección de Datos e Información (FDPIC), Suiza
- Comisión Nacional de Informática y Libertades (CNIL), Francia
- Unidad Reguladora y de Control de Datos Personales (URCDP), Uruguay
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), México
- Comisión de Acceso a la Información de Quebec, Canadá
- Comisionado de Información y Privacidad de Ontario, Canadá
- Oficina del Comisionado de Información y Privacidad de Columbia Británica, Canadá
- Oficina del Comisionado de Privacidad de Canadá
- Consejo de Europa
- Oficina del Comisionado de Privacidad de Datos Personales (PCPD), Hong Kong, China
- Comisión Nacional de Control de la Protección de Datos de Carácter Personal (CNDP), Marruecos
- Supervisor Europeo de Protección de Datos (EDPS)

La 45.ª Sesión Cerrada Anual de la Asamblea Global de Privacidad:

Observando que las actividades laborales pueden involucrar la búsqueda y contratación de candidatos, la formalización de un contrato de trabajo entre el empleador y el empleado, el monitoreo y gestión del desempeño, desarrollo y comportamiento de los empleados en el lugar de trabajo por parte del empleador, y la terminación de una relación laboral; y pueden incluir la contratación y gestión de trabajadores de plataformas (gig workers), empleados contractuales, sindicatos, así como el cuidado de la salud y seguridad en el trabajo y el cumplimiento de los requisitos laborales y de protección social;

Recordando la Declaración sobre Ética y Protección de Datos en la Inteligencia Artificial realizada por la 40.ª Conferencia Internacional de Comisionados de Protección de Datos y Privacidad el 23 de octubre de 2018, y la Resolución sobre Rendición de Cuentas en el Desarrollo y Uso de la Inteligencia Artificial adoptada en la 42.ª sesión cerrada de la conferencia de la GPA;

Reconociendo las eficiencias y beneficios potenciales para la escala de operaciones que el uso de la Inteligencia Artificial (IA) puede aportar a la toma de decisiones a lo largo del ciclo de vida laboral, que las organizaciones están explorando en diversas actividades impulsadas por el empleador, incluyendo, entre otras, la búsqueda inicial y el cribado de posibles candidatos a un puesto de trabajo, el monitoreo y la gestión de empleados;

Destacando que la IA utilizada en un contexto laboral puede representar un alto riesgo para las personas,[1] grupos, representantes de los trabajadores (como los sindicatos), comunidades y organizaciones. Cuando dicho uso es opaco, mal aplicado, diseñado incorrectamente o se depende de él de manera inapropiada, puede provocar daños o la vulneración de derechos y libertades fundamentales, incluyendo la privacidad, la dignidad humana y la igualdad de derechos, como la discriminación injusta. Esto puede impactar significativamente el desarrollo personal y profesional de un trabajador y resultar en la denegación de la igualdad de oportunidades para acceder al empleo debido al uso de datos históricos sesgados para entrenar algunas herramientas de IA o al uso de parámetros o valores inapropiados o ilícitos en el sistema de IA;

Destacando riesgos adicionales tales como la recopilación desproporcionada o no autorizada de datos personales para tomar decisiones únicamente automatizadas o asistidas por IA sobre el desempeño de un empleado o la asignación de trabajo, o cualquier otra decisión que también pueda afectar los derechos de las personas. Estos incluyen, entre otros:

- el derecho a la vida privada y familiar (por ejemplo, si los sistemas de IA se utilizan para monitorear a los trabajadores a domicilio o conllevan una microgestión excesiva de los trabajadores y vigilancia en el lugar de trabajo)
- la afectación negativa a la salud y el bienestar,
- la libertad de reunión y asociación (por ejemplo, si los datos o inferencias sobre la afiliación sindical se utilizan en detrimento de empleados o candidatos)
- la capacidad de una persona para ejercer su derecho a no ser sometida a una decisión basada total o parcialmente en la toma de decisiones automatizadas o para ejercer otros derechos individuales a la privacidad o la protección de datos, y
- la vulneración de los derechos individuales a la información y protección de datos, por ejemplo, cuando hay una falta de transparencia que implica que los candidatos o empleados no son conscientes del hecho de que se está utilizando IA y/o del alcance de su uso;

Reforzando la importancia de la transparencia para garantizar que los empleados y sindicatos sean informados sobre el uso de sistemas de IA en el lugar de trabajo antes de su introducción, proporcionando detalles suficientes para permitir que estos empleados y sindicatos comprendan su propósito, cómo funcionan y las métricas utilizadas;

Enfatizando que los sistemas de IA utilizados por las organizaciones para fines laborales deben ser explicables de una manera comprensible tanto para quienes están sujetos a decisiones tomadas únicamente o con la asistencia de esos sistemas, como para quienes utilizan los sistemas de IA. Las

[1] El riesgo puede evaluarse con referencia a herramientas como el Marco de Gestión de Riesgos de Inteligencia Artificial publicado por el Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST) a principios de este año, y la norma ISO/IEC 23894:2023 sobre Gestión de riesgos para la IA, entre otros. Véase también la propuesta del Grupo de Trabajo de IA de la Asamblea Global de Privacidad: "Riesgos para los Derechos y Libertades de las Personas Planteados por los Sistemas de Inteligencia Artificial – Propuesta para un Marco General de Gestión de Riesgos".

organizaciones que desplieguen tales sistemas, como parte central de sus responsabilidades de rendición de cuentas, así como de sus obligaciones bajo la legislación laboral, de protección social, de salud y seguridad aplicable, deben prever dicha explicabilidad y mecanismos, según se detallen en una política organizacional dedicada al uso de la IA. Los empleados, candidatos o trabajadores deben ser capaces de comprender la lógica del proceso de toma de decisiones a través de estos mecanismos y políticas, así como buscar ayuda y reparación en casos donde, por ejemplo, se observen problemas relacionados con la discriminación, el sesgo y la opacidad;

Observando que la mayoría de las aplicaciones de IA desarrolladas para o desplegadas en un contexto laboral procesarán datos personales en la fase de desarrollo o en la fase de despliegue. Si bien las fuentes, la distribución y la naturaleza de los datos procesados en esas diferentes etapas pueden diferir, todas las fases de dicha IA en el ciclo de vida laboral están, en la mayoría de los casos, vinculadas a consideraciones de protección de datos, privacidad y derechos laborales;

Preocupada porque el uso de la IA en el empleo puede conllevar altos riesgos para la protección de datos y la privacidad que pueden impactar, entre otros, en la contratación y el monitoreo de los trabajadores. Esos riesgos pueden incluir, entre otros:

- falta de transparencia
- presencia de patrones discriminatorios basados en sesgos
- falta de consideración sobre la necesidad y proporcionalidad del uso de la IA en el contexto laboral específico
- falta de intervención humana significativa
- falta de capacitación adecuada y experiencia relevante en la operación de sistemas de IA y en la gestión de la toma de decisiones de alto riesgo en el ecosistema laboral
- falta de una base legal válida, ya sea general o específica para el empleo
- pérdida de control de las personas sobre la recopilación y el procesamiento de sus datos personales
- dificultades enfrentadas por los empleados para ejercer sus derechos sobre los datos
- falta de salvaguardas específicas
- seguridad de datos deficiente
- extralimitación de funciones (*function creep*)
- el procesamiento de datos sensibles, como datos de salud o biométricos, sin respetar el principio de proporcionalidad o la dignidad humana;

Destacando que el uso de sistemas de IA para inferir emociones de una persona física,[2] y más generalmente cualquier forma de "categorización biométrica", es de alto riesgo y debería, en la mayoría de los casos, estar prohibido en el contexto laboral, y si se utiliza en casos limitados y definidos debe estar sujeto a salvaguardas apropiadas, incluyendo pruebas robustas y/u otras evaluaciones para asegurar que tales sistemas utilicen metodologías válidas y confiables y operen según lo previsto;

Enfatizando que, a medida que las organizaciones en los sectores privado y público dependen con más frecuencia de la IA en el contexto laboral, y que los sistemas y servicios de IA pueden proporcionarse de forma remota y transfronteriza, es importante que las autoridades de protección de datos y privacidad,

[2] Por ejemplo, en el caso de sistemas de reconocimiento de emociones utilizados en un lugar de trabajo para monitorear el estado de ánimo de los empleados.

junto con las autoridades competentes en materia laboral y de salud y seguridad, obtengan información sobre de dónde derivan los sistemas de IA sus datos de entrenamiento, cómo su desarrollo y operación cumplen con los marcos legales nacionales y cómo se ven afectados los derechos de protección de datos y privacidad de los empleados tanto a nivel nacional como internacional;

Observando las importantes contribuciones de las autoridades de protección de datos y privacidad, gobiernos y organismos internacionales al debate global a través de la publicación de leyes, políticas y documentos de orientación;

Reconociendo que los diferentes usos y aplicaciones de la IA en el empleo plantean diferentes tipos y niveles de riesgo y, por lo tanto, requieren una consideración cuidadosa a través de su despliegue y ciclo de vida para identificar las salvaguardas apropiadas en cada contexto y uso;

Recordando que la Asamblea Global de Privacidad ha identificado previamente la necesidad de trabajar hacia políticas, estándares y modelos globales, y de garantizar mayores niveles de cooperación regulatoria para mejorar la prevención, detección, disuasión y reparación eficiente de problemas de protección de datos y privacidad, así como para asegurar la coherencia y previsibilidad en el sistema de supervisión dentro de la economía impulsada por datos;

Afirmando la necesidad de que las autoridades de control de protección de datos y privacidad coordinen sus esfuerzos, junto con las autoridades competentes en materia laboral y de salud y seguridad, para influir en el desarrollo e implementación de estos enfoques de protección de datos y privacidad en todo el mundo, y para tomar medidas cuando sea apropiado; y

Reafirmando la Resolución sobre Privacidad desde el Diseño adoptada por la 32.ª Conferencia en 2010 en Jerusalén, la Resolución sobre la Elaboración de Perfiles adoptada por la 35.ª Conferencia en 2013 en Varsovia, la Resolución sobre Big Data adoptada por la 36.ª Conferencia en 2014 en Fort Balaclava, la Declaración sobre Ética y Protección de Datos en la IA adoptada por la 40.ª Asamblea Global de Privacidad en 2018 en Bruselas, y la Resolución sobre Rendición de Cuentas en el Desarrollo y Uso de la IA adoptada por la 42.ª Asamblea Global de Privacidad en 2020 de forma virtual.

Por lo tanto, la 45.ª Asamblea Global de Privacidad subraya la importancia de:

1. Garantizar que el uso de sistemas de IA en un contexto laboral esté centrado en el ser humano.

2. Los principios de protección de datos y privacidad desde el diseño y por defecto en el desarrollo de herramientas de IA para su despliegue en contextos laborales, incluyendo, entre otros, a empleados, trabajadores contractuales, trabajadores sindicalizados, jornaleros y trabajadores de plataformas (*gig workers*), reconociendo el impacto que los sistemas de IA pueden tener en sus vidas personales y profesionales.

3. Reconocer la importancia de contar con una base jurídica adecuada para el tratamiento de datos personales en todas las fases del ciclo de vida de la IA, y las limitaciones del consentimiento como base legal en el contexto laboral dada la asimetría de poder entre un candidato o empleado y el empleador.

4. Detallar salvaguardas adecuadas para evitar la vigilancia desproporcionada de los trabajadores en violación de la privacidad y dignidad de los empleados al tratar sus datos personales para el propósito relevante del trabajo a realizar, incluyendo la participación de los sindicatos en las decisiones sobre la gestión del trabajo mediante IA.

5. La necesidad de un cumplimiento pleno del desarrollo y despliegue de sistemas de IA en el empleo con las leyes y principios de protección de datos aplicables, tales como necesidad, proporcionalidad, minimización de datos, especificación y limitación de la finalidad, y el derecho a no ser objeto de una decisión basada únicamente o principalmente en medios automatizados; así como con las regulaciones laborales pertinentes y cualquier otra normativa, como los marcos de derechos humanos establecidos, que puedan tener relevancia en un contexto específico, incluyendo, entre otros, los principios mencionados en esta resolución.

6. Licitud, lealtad y transparencia en relación con la forma en que se tratan los datos personales, incluyendo el desarrollo, el despliegue y el resultado de dicho tratamiento relacionado con la IA. Esto implica, entre otras cosas, la obligación del empleador de proporcionar al empleado —sujeto de una decisión asistida por IA cuando se despliegan sistemas algorítmicos o de IA en el contexto laboral con respecto a los marcos regulatorios específicos de cada jurisdicción— y al sindicato, antes del despliegue de cualquier sistema de IA, información detallada sobre el uso y funcionamiento de tales sistemas que determinen, por ejemplo, la clasificación de un candidato o empleado, la asignación de tareas, la gestión o el despido, así como la supervisión, evaluación y desempeño de las obligaciones contractuales del empleado, sin perjuicio de los derechos de los trabajadores, por ejemplo, a recibir información relacionada con el empleo, a impugnar y buscar reparación por una evaluación de desempeño ilegal, pagos insuficientes y despidos improcedentes.

7. El derecho de un candidato o empleado que es objeto de una decisión asistida por IA a acceder a la información sobre qué datos posee el empleador sobre él y cómo se utilizan sus datos personales en relación con dicha decisión asistida por IA, así como información sobre los datos que se infieren y los perfiles que se crean utilizando estos sistemas de IA.

8. La explicabilidad del sistema de IA utilizado en cualquier etapa del ciclo de vida laboral para garantizar que los empleados, candidatos o trabajadores afectados por el resultado de dicho sistema, así como los empleadores que lo despliegan, comprendan la decisión tomada con el sistema de IA y puedan acceder a esa explicación de manera sencilla y oportuna; y que la explicación para los empleados, candidatos o trabajadores incluya información inteligible sobre la lógica aplicada, la importancia y las consecuencias previstas del uso del sistema de IA, tanto en general como en el caso específico del empleado, para asegurar que puedan presentar quejas informadas y ejercer su derecho a la reparación de acuerdo con el marco legal nacional aplicable.

9. La capacidad del interesado afectado por un sistema de IA utilizado por un empleador en cualquier etapa del ciclo de vida laboral de obtener una revisión humana registrada y significativa de las decisiones laborales tomadas mediante sistemas de IA, de expresar su punto de vista y de impugnar las decisiones automatizadas o basadas en IA pertinentes, o de solicitar una auditoría independiente de un sistema de IA utilizado por el empleador o cualquier requisito general de auditoría por terceros.

10. Capacitar a los usuarios de herramientas de IA, incluyendo a quienes realizan la revisión humana de decisiones asistidas por IA, para asegurar que dichas decisiones no estén sujetas al sesgo de automatización que podría llevar a una confianza excesiva en las herramientas de IA, y que los usuarios de estas herramientas tengan la pericia, experiencia y calificaciones técnicas necesarias y consideren los niveles de riesgo de la tarea influenciada por el resultado del sistema de IA; así como rastrear o monitorear el uso de las herramientas de IA para determinar si dicha capacitación es efectiva.

11. La rendición de cuentas como principio, que exige que las organizaciones y los empleadores tengan en cuenta, mitiguen y, cuando sea necesario, prevengan los riesgos para los derechos y

libertades de los candidatos, empleados y trabajadores derivados del uso de la IA para tratar datos personales (por ejemplo, el derecho de asociación y a organizarse en un sindicato, que puede verse obstaculizado por un monitoreo indebido de las actividades de los trabajadores), y demuestren que lo han hecho.

12. Políticas organizacionales que respalden evaluaciones de impacto de la IA previas al despliegue, teniendo en cuenta todos los riesgos razonablemente previsibles para los candidatos, empleados y trabajadores derivados del uso del sistema de IA en el lugar de trabajo, la acreditación o certificación de los sistemas de IA, la identificación de riesgos específicos de la IA y el diseño de mecanismos de denuncia (*whistleblowing*) y reparación para los sistemas de IA utilizados durante el ciclo de vida laboral, también como medio para facilitar la supervisión por parte de las autoridades competentes.

13. Reducir y mitigar los sesgos o la discriminación, tanto directa como indirecta, al desarrollar y desplegar un sistema de IA en el contexto laboral, incluso tomando medidas razonables para asegurar que los datos personales utilizados en el entrenamiento de un sistema y en la toma de decisiones únicamente automatizada sean representativos del contexto en el que se utilizará el sistema, sean precisos y se actualicen regularmente; e implementar medidas técnicas y organizativas apropiadas para asegurar, en particular, que se corrijan los factores en los sistemas de contratación y gestión laboral que den lugar a inexactitudes en los datos personales y se minimice el riesgo de errores, así como el cumplimiento de las leyes nacionales aplicables.

La 45.ª Asamblea Global de Privacidad resuelve:

1. **Urgir** a las organizaciones que desarrollan o utilizan sistemas de IA para su uso en el contexto laboral a tener en cuenta las consideraciones descritas en esta resolución;

2. **Hacer un llamado** a todos los miembros de la Asamblea Global de Privacidad para que trabajen con las organizaciones que desarrollan o utilizan sistemas de IA en el contexto laboral, tanto en sus jurisdicciones como a nivel mundial, para ayudarlas a incorporar las consideraciones descritas en esta resolución;

3. **Actualizar**, cuando sea apropiado, los resultados de la encuesta del Grupo de Trabajo sobre Ética y Protección de Datos en la Inteligencia Artificial (véase el informe de la encuesta en la Nota Explicativa a continuación) en caso de posibles cambios en el panorama legal o técnico del uso de la IA en el empleo.

NOTA EXPLICATIVA

El GRUPO DE TRABAJO DE LA ASAMBLEA GLOBAL DE PRIVACIDAD SOBRE ÉTICA Y PROTECCIÓN DE DATOS EN LA INTELIGENCIA ARTIFICIAL llevó a cabo una encuesta entre mayo y julio de 2022 para recopilar las opiniones de los miembros de la Asamblea Global de Privacidad sobre los riesgos clave y las acciones de supervisión que los miembros han tomado en relación con el uso de la IA en el ámbito laboral. El informe se presenta a continuación.

1. Introducción

En los últimos años se ha observado una proliferación en el uso de la inteligencia artificial (IA) en el empleo, incluyendo su utilización en procesos de selección, en el lugar de trabajo y tras el fin de la relación laboral. La IA es un término general que abarca una variedad de tecnologías y enfoques que a menudo intentan imitar el pensamiento humano para resolver tareas complejas.[3] El término "IA" suele utilizarse para describir todo tipo de herramientas algorítmicas disponibles en el mercado sin una definición concreta, lo que puede conducir al fenómeno del "*AI washing*". Desde la perspectiva de la protección de datos, es importante distinguir entre la fase de concepción o entrenamiento y la fase de aplicación o despliegue de la IA en el contexto laboral. La mayoría de las aplicaciones de IA en este ámbito usarán datos personales en ambas fases, por lo que las consideraciones sobre protección de datos y privacidad resultan aplicables. Estas consideraciones incluyen, entre otras, cuestiones de transparencia como la exactitud de los datos sobre empleados, trabajadores y candidatos; preguntas relacionadas con la garantía de los derechos de los interesados y las salvaguardas pertinentes; la presencia de sesgos y discriminación; las bases jurídicas o el grado de intervención humana significativa; así como proporcionalidad, confianza y equidad.

En 2018 se informó de que Amazon había descartado una herramienta de reclutamiento impulsada por inteligencia artificial que utilizaba tras evidenciarse que mostraba sesgo contra las mujeres. La herramienta había sido diseñada para evaluar y puntuar solicitudes de empleo. Sin embargo, se alegó que el sistema de IA penalizaba solicitudes que incluyeran la palabra "women's" (femenino), como en "women's chess club captain" (capitana del club de ajedrez femenino), y bajaba la puntuación de las graduadas de dos universidades exclusivamente femeninas. Este fue uno de los primeros casos publicitados que mostró no solo que la IA se utilizaba para tomar decisiones importantes en un contexto laboral, sino que además estaba generando perjuicios injustificados para las personas.

Desde entonces, ha habido más casos de gran repercusión donde la IA se ha utilizado en el ámbito laboral y ha producido posibles daños a individuos. Algunos ejemplos incluyen:

- Una sentencia de un tribunal neerlandés sobre si la desactivación de las licencias de algunos conductores de Uber constituía una decisión tomada únicamente de forma automatizada con efectos legales o significativamente similares según el artículo 22 del RGPD, y si se proporcionó a los conductores información significativa sobre la lógica utilizada para tomar la decisión.[4]

La autoridad supervisora italiana (Garante) impuso multas a empresas de reparto de comida por infringir los principios de transparencia, seguridad, privacidad desde el diseño y por defecto, y por no implementar medidas adecuadas para salvaguardar los derechos y libertades de sus empleados frente a decisiones automatizadas discriminatorias cuando utilizaban un sistema automatizado de puntuación

[3] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/part-1-the-basics-of-explaining-ai/ (un conjunto de directrices, ICO, UK)
[4] Dutch court rulings break new ground on gig worker data rights | Financial Times (ft.com)

para asignar franjas de entrega a repartidores, lo que excluyó a algunos de oportunidades laborales.[5]

Los legisladores y reguladores han empezado a abordar los posibles daños derivados del uso de la IA en el ámbito laboral. Por ejemplo, la Comisión Europea ha propuesto considerar como de alto riesgo el uso de IA para la contratación, así como para decisiones relacionadas con el rendimiento laboral y la asignación de tareas; además, se está negociando una propuesta relativa a los trabajadores de plataformas digitales.[6] Esto significaría que los empleadores deberán cumplir requisitos adicionales conforme a la Ley de IA en comparación con otros usuarios de sistemas de IA que no se consideran de alto riesgo. La Oficina del Comisionado de Información (ICO), la autoridad de protección de datos del Reino Unido, se ha comprometido a investigar las preocupaciones sobre el uso de algoritmos para filtrar solicitudes de empleo que podrían estar afectando negativamente las oportunidades laborales de personas de diversos orígenes.

Muchas aplicaciones de IA utilizadas en el ámbito laboral tendrán implicaciones para la protección de datos y la privacidad. Por ejemplo:

- ¿Podrá explicarse a las personas afectadas una decisión derivada de IA sobre si un candidato es seleccionado o no?
- ¿Se utilizará un sistema de IA diseñado para un propósito (p. ej., aumentar la seguridad de los empleados en el lugar de trabajo) para un fin separado e incompatible (p. ej., puntuar la productividad de los trabajadores)?
- ¿Puede considerarse justa alguna vez la decisión de un sistema de IA de despedir a un empleado?

En 2022, la Asamblea Global de Privacidad (GPA), liderada por la ICO y el BfDI de Alemania, realizó una encuesta entre sus miembros para entender las perspectivas globales sobre las implicaciones para la protección de datos y la privacidad derivadas de la IA en el contexto laboral. Los objetivos de la encuesta fueron:

- Identificar cuestiones clave de política y jurídicas relacionadas con el desarrollo y uso de la IA en el ámbito laboral, incluida la contratación, que resulten importantes para las autoridades de protección de datos y privacidad de todo el mundo.
- Reunir y mantener un repositorio internacional de casos reales de aplicaciones de tecnologías de IA en el lugar de trabajo, relevantes para considerar la privacidad, la protección de datos y la ética de la IA de forma más amplia.
- Informar el desarrollo y la promoción de un conjunto de principios y expectativas para el uso de la IA y la información personal en el ámbito laboral.
- Considerar y debatir posibles líneas de acción.

La encuesta preguntó sobre las posiciones políticas y directrices existentes de las autoridades de protección de datos acerca del uso de datos personales y IA en el lugar de trabajo (pregunta 1), información sobre acciones de cumplimiento o investigaciones relacionadas (pregunta 2), en qué medida los miembros interactuaban con partes interesadas y qué consideraban los usos más riesgosos de la IA en el trabajo (preguntas 3 y 4), cuáles consideraban los mayores riesgos para la privacidad y la protección de datos (pregunta 5), y cómo sería un marco regulatorio eficaz (pregunta 6). Finalmente, la encuesta

[5] Véase el resumen de la orden de la Autoridad Italiana de Protección de Datos en https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677611; otra decisión está publicada en https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685994.

[6] Digital platform workers: EU rules one step closer (europa.eu)

pidió ejemplos de usos de IA en el entorno laboral (pregunta 7) y áreas de impacto más amplias (pregunta 8).

La encuesta se realizó del 11 al 25 de mayo de 2022 y las preguntas fueron difundidas por correo electrónico por la secretaría de la GPA para el Grupo de Trabajo de Ética y Protección de Datos en la Inteligencia Artificial, acompañadas de una nota introductoria. Para maximizar el número de respuestas, la encuesta se envió a todos los miembros de la GPA en general, y no solo a los integrantes del Grupo de Trabajo sobre Ética y Protección de Datos en IA. En total, se recibieron 29 respuestas de miembros de la GPA. La mayoría procedía de autoridades ubicadas geográficamente en Europa (20/29), seguidas por Asia y Australia (6/29), América del Norte (1/29) y América Central y del Sur (2/29).

2. Resultados

La encuesta dio lugar a una variedad de respuestas por parte de las autoridades de protección de datos y privacidad. Las preguntas y un resumen de las respuestas recibidas se presentan a continuación.

Pregunta uno: ¿Ha desarrollado su autoridad alguna posición política pública o guía sobre el uso de datos personales e IA en el lugar de trabajo?

En total, ocho encuestados respondieron "sí" a esta pregunta. La información adicional proporcionada mostró una variedad de publicaciones diferentes. Por ejemplo, algunas se centraban en los riesgos generales asociados al uso de IA, otras en los riesgos generales del tratamiento de datos personales en el contexto laboral, y finalmente hubo varios ejemplos centrados específicamente en el uso de datos personales e IA en el lugar de trabajo. Por ejemplo, una respuesta destacó las consideraciones necesarias al intentar conciliar el principio de minimización de datos con el principio de equidad cuando el método para detectar y contrarrestar la discriminación requiere tratar más datos personales.

Pregunta dos: ¿Ha investigado su autoridad, u otros organismos legales o judiciales en su jurisdicción, o tomado medidas regulatorias, de cumplimiento o legales formales respecto al uso de datos personales e IA en el lugar de trabajo?

Ocho encuestados respondieron "sí" a esta pregunta. Algunos ejemplos incluidos fueron:

- Investigaciones a empresas de reparto de comida online y cómo utilizan IA para tratar los datos personales de los conductores.
- El tratamiento de datos personales de empleados mediante técnicas avanzadas de minería de datos con el fin de identificar posibles bajas médicas injustificadas.
- El uso de toma de decisiones basadas en algoritmos para asignar puestos docentes en escuelas.
- El uso de análisis automático de voz e imagen durante entrevistas por vídeo como parte de un proceso de selección.
- El uso de biometría en el lugar de trabajo; y
- El uso de IA para analizar datos y predecir la probabilidad de que un candidato rechace una oferta de trabajo.

Pregunta tres: ¿Ha colaborado su autoridad con partes interesadas externas a nivel regional, nacional o internacional en el desarrollo de posiciones políticas, guías o acciones regulatorias sobre el uso de la IA en el lugar de trabajo (por ejemplo, industria, sindicatos, sociedad civil, legisladores)?

Once encuestados respondieron "sí". La colaboración incluyó participación en foros internacionales como el Comité Ad Hoc del Consejo de Europa sobre Inteligencia Artificial, la OCDE y la Alianza Global

para la IA, así como con otras autoridades y reguladores nacionales, empresas y organismos sectoriales, instituciones de investigación, sindicatos, sociedad civil y departamentos y ministerios gubernamentales nacionales.

Pregunta cuatro:

De la siguiente lista de casos de uso, ¿cuáles considera que plantean los mayores riesgos para la privacidad y la protección de datos?

- Fines de contratación (p. ej., extracción de CV, evaluaciones gamificadas, entrevistas automatizadas, etc.)
- Fines de gestión laboral (p. ej., asignación de vacaciones, gestión de ausencias, asignación de tareas y turnos, etc.)
- Fines de monitorización (p. ej., verificación de identidad, sistemas de rastreo, monitorización de ordenadores, etc.)
- Otros (especifique)

Los encuestados pudieron elegir múltiples respuestas; muchos seleccionaron dos o tres, algunos eligieron solo una y un par optó por abstenerse de responder. Las autoridades de protección de datos consideraron que el uso de la IA con fines de monitoreo representa el mayor riesgo para la privacidad y la protección de datos, seguido de cerca por el uso de la IA con fines de contratación. Algunos encuestados que seleccionaron "Otros" consideraron que los tres usos planteaban un nivel de riesgo similar.

Además, catorce encuestados mencionaron otros propósitos y/o agregaron contenido adicional en su respuesta. Entre ellos, se señaló que los riesgos dependían del grado de infracción de los derechos de privacidad y las libertades de los interesados, en lugar del escenario específico en el contexto laboral o un propósito concreto. Algunos atribuyeron un alto riesgo a la vigilancia permanente con tecnologías de reconocimiento facial mediante IA, especialmente en torno a la inclusión de datos sensibles como la biométrica, por ejemplo, para fines de identificación o elaboración de perfiles automatizados de empleados. Hubo preocupación por la falta de pruebas científicas de las afirmaciones y promesas hechas por los vendedores de dichas herramientas, incluidas las predicciones sobre el carácter y el desempeño de los candidatos que no se basan en métodos científicos de calidad controlada. Con frecuencia, los encuestados consideraron que los conjuntos de datos de entrenamiento no se obtienen ni se procesan de forma que cumplan con la protección de datos. También mencionaron inquietudes sobre la gobernanza y la seguridad de las bases de datos como fuentes de los datos que la IA recopila. Además, los encuestados subrayaron que, además de una evaluación de riesgos concreta, debe existir una base jurídica válida y deben respetarse los principios de protección de datos en cualquier caso (i.e., minimización de datos, transparencia, equidad/no discriminación y la necesidad de que el uso de la IA en el lugar de trabajo sea proporcionado en relación con el propósito concreto, etc.). Los encuestados también mencionaron la necesidad de salvaguardias específicas.

Pregunta cinco: Para los casos de uso identificados en la pregunta cuatro, seleccione los que considere los tres riesgos más significativos para la privacidad y la protección de datos.

- **Falta de transparencia respecto a la recogida de datos, incluida la falta de suministro de información a las personas.**
- **Recopilación a gran escala de categorías especiales de datos.**
- **Sesgo y discriminación contra ciertos grupos demográficos.**
- **Deficiente seguridad de los datos, incluyendo posibles violaciones de la confidencialidad.**
- **Extensión de funciones (uso posterior de un sistema de IA en el lugar de trabajo para fines nuevos, potencialmente menos convincentes).**
- **Pérdida de control de las personas sobre la recogida y el tratamiento de los datos.**
- **Falta de base jurídica válida para el tratamiento.**
- **Dificultad de las personas para ejercer sus derechos en materia de datos.**
- **Falta de leyes específicas que regulen el uso de la IA en el lugar de trabajo.**
- **Falta de consideración sobre la necesidad y la proporcionalidad del uso de la IA en el lugar de trabajo.**
- **Falta de intervención humana significativa en las decisiones tomadas que tengan efectos jurídicos o significativamente similares en las personas.**
- **Implicaciones más amplias para los derechos humanos, tal como se establecen en instrumentos internacionales como el Pacto Internacional de Derechos Económicos, Sociales y Culturales o la legislación nacional, incluido el derecho de libertad de reunión y asociación.**
- **Otros (especifique).**

La mayoría de las autoridades de protección de datos consideraron que la falta de transparencia constituye el mayor riesgo para la protección de datos y la privacidad (15 encuestados). A esto le siguieron el sesgo y la discriminación (10 encuestados), la falta de consideración sobre la necesidad y proporcionalidad del uso de la IA en el lugar de trabajo (9 encuestados) y la falta de intervención humana significativa (8 encuestados). Algunos encuestados también seleccionaron "falta de base jurídica válida" (6 encuestados) y "falta de leyes específicas que regulen el uso de la IA en el lugar de trabajo" (5 encuestados). Otros seleccionaron la dificultad de las personas para ejercer sus derechos en materia de datos (3 encuestados) y la pérdida de control de las personas sobre la recogida y el tratamiento de los datos (5 encuestados).

Varios encuestados también mencionaron la deficiente seguridad de los datos (5) y la extensión de funciones (4). El riesgo de recopilación a gran escala de categorías especiales de datos se mencionó una vez. Ninguno de los encuestados seleccionó "implicaciones más amplias para los derechos humanos".

Pregunta seis: ¿Cómo sería un marco regulatorio eficaz para la IA en el lugar de trabajo?

Los encuestados ofrecieron diversas sugerencias sobre cómo sería un marco regulatorio eficaz para la IA en el entorno laboral. Muchas autoridades (18) sugirieron una nueva regulación legal o señalaron iniciativas legales existentes o futuras en sus países/continentes aplicables a la IA en el contexto del empleo. Varias autoridades (10) sugirieron, adicional o exclusivamente, el uso de "derecho blando" (*soft law*), como directrices o educación. Algunas de las sugerencias indicativas y no exhaustivas proporcionadas fueron:

- **Regulación legal específica** para el uso de la IA en el lugar de trabajo, que incluya, por ejemplo, definiciones, clasificaciones de riesgo, protección de datos desde el diseño y por defecto, y restricciones al desarrollo y/o uso de la IA en el trabajo, como la limitación de la finalidad.
- Garantizar que los sistemas de IA utilizados para **decisiones laborales significativas sean explicables.**
- Las organizaciones deben ser transparentes y responsables sobre su uso de la IA en el trabajo para permitir que las personas ejerzan una elección y un control significativos en relación con sus datos personales.
- Requisitos para que los sistemas de IA y su uso por parte de los empleadores estén sujetos a **auditorías de terceros u otra forma de escrutinio externo**, **incluso antes de su despliegue**.
- Asegurar que el marco regulatorio para la IA en el trabajo sea coherente y compatible con **el derecho laboral y los convenios colectivos.**
- Capacidad de los **representantes de los trabajadores para solicitar información** sobre los sistemas algorítmicos.
- **Cumplimiento del artículo 22 del RGPD donde sea aplicable o restricciones similares** sobre la toma de decisiones automatizada en el contexto del empleo.
- Clasificar ciertos usos de la IA en el empleo como de alto riesgo, y prohibir ciertos sistemas donde exista un riesgo alto no mitigado, como sesgos injustos y discriminación, para facilitar la aplicación de la ley.
- **Restringir algunos usos de la IA y prohibir otros** que planteen **riesgos altos o inaceptables para la privacidad individual** (por ejemplo, sistemas de identificación biométrica automatizada para la calificación social basada en IA). Restricciones legales donde falte una base jurídica para el tratamiento de datos personales en el empleo, no haya proporcionalidad respecto a los fines y sea difícil encontrar medidas para mitigar los riesgos elevados, a fin de proteger las libertades y derechos de los interesados.
- **Seguridad jurídica, protección y ejercicio efectivo de los derechos individuales de protección de datos y privacidad de los candidatos y empleados**. Para que las personas puedan ejercer un control real sobre su información, las empresas primero deben operar con transparencia y rendición de cuentas, y hacer que la IA sea comprensible.
- **Salvaguardias adecuadas** previstas por la ley y a través de marcos regulatorios, *soft law* y herramientas prácticas (guías), medidas de autorregulación en las empresas, etc.
- El requisito de que la IA sea razonablemente necesaria para las funciones o actividades de una entidad a fin de cumplir con el **principio de proporcionalidad**. Por ejemplo, esto podría ponderarse considerando el grado de sensibilidad de los datos personales involucrados, la legitimidad del propósito de la organización, la existencia de medios menos invasivos y la proporcionalidad entre la pérdida de privacidad y los beneficios obtenidos.
- Deben existir restricciones para garantizar que los **datos de entrenamiento** para los sistemas

de IA en el empleo se obtengan y procesen de manera legal y transparente.

- Declaración clara de los usos aceptables de la IA en el lugar de trabajo, garantizando un uso seguro, ético y práctico.

Pregunta siete: Resuma brevemente ejemplos de usos de la IA en el lugar de trabajo en la práctica dentro de su jurisdicción.

Varias autoridades destacaron el uso de la IA en la selección de personal, desde el filtrado de CV hasta el análisis de entrevistas en vídeo, la realización de verificaciones de antecedentes mediante reconocimiento facial y comparaciones fotográficas en redes sociales, elaboración de perfiles a gran escala desde múltiples fuentes de datos y el uso de juegos para filtrar candidatos. Algunos observaron casos en los que el software de preselección y clasificación dio lugar a discriminación. Otros también señalaron la IA utilizada para monitorear empleados, como el rastreo de vehículos y dispositivos móviles, el uso de cámaras web con IA para supervisar a quienes trabajan desde casa o el monitoreo de pulsaciones de teclas. También hubo menciones al uso de IA para medir el rendimiento individual, evaluar el bienestar o la salud de los empleados y detectar bajas por enfermedad injustificadas mediante técnicas de minería de datos. Algunos observaron el uso de datos biométricos para el control de acceso, control horario o análisis de rasgos de personalidad, así como videovigilancia con reconocimiento facial en accesos. Otros detectaron software de videoconferencia con algoritmos de IA sin base legal adecuada, y señalaron que las redes sociales profesionales dependen en gran medida de algoritmos de emparejamiento y selección.

Pregunta ocho: ¿Ha identificado áreas de impacto más amplias en torno al uso de la IA en el empleo que desee plantear (impacto en consumidores, competencia, cumplimiento de la legislación laboral, etc.)?

Diversas autoridades destacaron la necesidad de compatibilidad con otros marcos legales, como el derecho del consumo y el derecho laboral, así como la preocupación por la desigualdad y la discriminación injusta a gran escala.