Posicionamiento personal sobre el impacto del tratamiento masivo de datos en las relaciones laborales. ¿Herramienta de "objetivización"?

La tecnología, por su propia idiosincrasia, es neutral, no posee cualidades humanas que le hagan actuar de forma subjetiva. La clave no está tanto en el proceso decisorio sino en las series de datos que alimentan las decisiones automatizadas; que dichos algoritmos de decisión estén siendo entrenados con datos que NO contengan patrones de sesgo. O, dicho de otra forma, si confiamos que todo proceso tecnológico basado en algoritmos es directamente "objetivo" podemos estar ante el peligro de crear una suerte de Intolerancia artificial. De hecho, el RGPD ya prevé esta circunstancia al afirmar que: "Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar", en una clara caución ante posibles sesgos de entrada en los algoritmos de decisión.

Las aplicaciones teóricas sobre el ámbito laboral de decisiones, parcial o totalmente, automatizadas, son muchísimas: reclutamiento, promoción, ascensos, incentivos, sanciones; y todas ellas deben estar exentas de patrones de sesgo, situaciones discriminatorias o que atenten contra la igualdad de oportunidades. Existen varios ejemplos de algoritmos con funcionamiento inadmisible: como Google Photos, que confundía fotos de simios con personas negras[1], o el algoritmo de reclutamiento de IBM en los años 90, que discriminaba a las mujeres[2]. Por eso el Reglamento prevé que se tenga que proporcionar "información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado", siempre al objeto de verificar si su funcionamiento es conforme a derecho.

Por tanto, la pregunta que se plantea sería: ¿cómo accedemos y comprendemos el funcionamiento de estos procesos algorítmicos sin romper el secreto industrial? Los algoritmos actúan como "cajas negras" a las que no todo el mundo puede tener acceso – ni todo el mundo puede entender e interpretar- y que contienen patentes susceptibles de ser violadas si son accesibles de forma generalizada. ¿Cómo compatibilizamos secreto industrial y acceso a los algoritmos decisorios?

Además, y ante este escenario, susceptible de ser sumamente litigioso, ¿estamos seguros de quién tendría la carga de la prueba en un conflicto por posible discriminación en una decisión automatizada? ¿Quién debe demostrar la parcialidad o imparcialidad de un algoritmo; la empresa que lo usa o el empleado sobre el que se ejerce la decisión automatizada?

Desde mi punto de vista, la solución vendrá dada por empresas auditoras que verifiquen/periten el comportamiento adecuado de estos algoritmos. Por ejemplo, la ya citada IBM, a través de su programa *Trust and Compliance*, tiene la capacidad comprobar el comportamiento de cualquier

---

[1] https://elpais.com/tecnologia/2018/01/14/actualidad/1515955554_803955.html

[2] https://www.businessinsider.com/sc/how-bias-pushed-the-computer-girls-out-of-tech-2018-4?IR=T

plataforma de inteligencia artificial analizando el set de datos que se ha usado para entrenar estos algoritmos. Verifica si los datos están siendo demasiado sesgados hacia uno u otro lado o si la muestra es lo suficientemente amplia y significativa para ser veraz y plural, y por lo tanto, realmente objetiva.

¿Qué buenas prácticas serían recomendables en el establecimiento de un sistema de control de la actividad laboral? (Artículos 89 y 90 del Proyecto LOPD)

Desde mi punto de vista, todas aquellas que pasen por el artículo 91, referente a los Derechos digitales en la negociación colectiva.

Aconsejo ejercer un amplio Diálogo Social con la Representación de los Trabajadores, poniendo en primer plano la negociación colectiva y la búsqueda del consenso a través de la explicación detallada, directa y honesta del proyecto, con absoluta transparencia, con vocación de respeto por los derechos de los trabajadores, acompañado de un plan de prevención de riesgos físicos y psicológicos, y con el máximo respeto a la conciliación de la vida personal y laboral.

O desde otro punto de vista, evitar tentaciones ejecutivas u obligatorias. Cualquier proceso de control de la actividad laboral derivado de la aplicación de nuevas tecnologías que se efectúe sin acuerdo con los trabajadores acarreará un proceso de litigiosidad incompatible con la viabilidad del proyecto. Y por último, lograr la implicación de los afectados en su puesta en marcha y desarrollo, porque si no, el proyecto estará abocado al fracaso.

Para evitar estos procesos de imposición y como guía de implementación de estos proyectos tecnológicos de control de la actividad laboral, en UGT estamos trabajando en un Test de verificación, que constaría de 3 partes:

Una evaluación empresarial de la pertinencia del proyecto, en términos de laboralidad, legitimidad, propósito, finalidad, proporcionalidad, idoneidad e intrusividad.

Un *checklist* de comprobación de la observancia de los derechos de los trabajadores desde un punto de vista colectivo e individual (información y consulta, derechos ARCO, tratamiento anonimizado, contenido del consentimiento informado, derechos fundamentales -intimidad, privacidad, dignidad, honor, integridad, secreto de las comunicaciones-, evaluación de riesgos psicosociales, venta de los datos a terceros)

Y, para finalizar, una serie de Recomendaciones para alcanzar la implicación de los trabajadores (alcanzar un Acuerdo Colectivo con cautelas sobre el impacto en el empleo, la mejora de la conciliación de la vida personal y profesional y sobre la aplicación del régimen disciplinario, así como directrices para la puesta en marcha del Derecho a la Desconexión y recomendaciones sobre la propiedad de los dispositivos que entran en el ámbito del control empresarial).

¿Existen las condiciones adecuadas para que el Big Data permita una mejora sustancial de las herramientas de prevención de riesgos laborales y de vigilancia de la salud?

Tecnológicamente sí, hay soluciones que ayudarían a mejorar la salud de los trabajadores de forma muy relevante. Y si a la propia *big data* le añadiésemos la *sensónica*, con por ejemplo con proyectos de pulseras que miden las pulsaciones o la tensión arterial, los beneficios para la salud podrían ser exponenciales.

La cuestión es si existe el clima necesario desde un punto de vista de confianza, o dicho de otra forma, si dicho uso de la tecnología tendría como consecuencia una merma de la privacidad del trabajador/paciente. Lamentablemente, considero que hoy no existe ese clima propiciatorio: los antecedentes generales no son buenos, y las malas prácticas detectadas han enturbiado la percepción. Socialmente, bajo mi punto de vista, no existen las condiciones adecuadas para que el big data y la algorítmica se apliquen sobre la vigilancia de la salud en el entorno laboral.

No podemos olvidar que estamos frente a un negocio: los datos son objeto de comercio permanentemente. Y los antecedentes sobre la ética y el modo de tratar nuestros datos por parte de algunos actores, no invitan al optimismo.

Los trabajadores somos generadores natos de datos y, por tanto, generamos materia prima con la comerciar; datos por otra parte muy valiosos, puesto que los relacionados con la salud son más escasos y por tanto, más atractivos comercialmente. Y eso entraña tentación, y por ende, peligros de intromisión, alteración de la privacidad y comercio ilegítimo de datos de los trabajadores que no están suficientemente resueltos en la actualidad.

¿Qué limitaciones tiene el uso de datos biométricos en el entorno laboral? (huella dactilar, iris, etc.)

Aquellos que delimita la propia laboralidad y la minimización de la intrusión. Es decir, ¿el proyecto de medida tiene una relación directa e inequívoca con la actividad laboral (actividad que realiza la empresa y con la prestación de servicios que efectúan los trabajadores), y por otro lado, ¿es pertinente y está justificado? ¿existe una alternativa menos intrusiva?

Por ahora existen pocos ejemplos en donde este binomio de laboralidad-intrusividad se sustente y se pueda llevar a la práctica con éxito, más allá de ciertas experiencias mediáticas de dudoso gusto y legalidad, como por ejemplo los chips subcutáneos: son altamente invasivos y su uso es trivial (control de la impresora y de acceso a las instalaciones).

Por tanto, hasta que existan soluciones que aporten algo nuevo (una aplicación nueva que no conocemos, lo que los expertos denominan una *killer app*) y que cumplan con la relación de

laboralidad/intrusividad, no espero una explosión en el uso de los datos biométricos en el entorno laboral.

¿Qué *skills* consideráis que debemos desarrollar los laboralistas para afrontar los retos que plantea el Big Data?

La pregunta es todo un desafío, mitad intelectual mitad adivinatoria.

Pero si miramos las tendencias generales para el empleo del futuro, y aplicándolas a vuestra profesión, deberíamos decir que un laboralista, dentro de 5 años debería acreditar:

En primer lugar, una altísima cualificación en su especialización profesional.

A la que debe añadir: unas habilidades digitales medias y altas, no solo para comprender las nuevas tendencias del trabajo y las soluciones tecnológicas que aplican los clientes, sino también para manejar herramientas que le ayuden en su rutina diaria (como la IA); y unas nuevas competencias transversales, que lo distingan de los demás abogados (ya sean humanos o cibernéticos) como la creatividad, la empatía, la comunicación o el pensamiento crítico.

Y todas ellas, en permanente actualización (el archiconocido *lifelong learning*) para no perder su vigencia.

Eva María Blázquez Agudo

Profesora Titular de Derecho del Trabajo y de la Seguridad Social

evamaria.blazquez@uc3m.es

Posicionamiento personal sobre el impacto del tratamiento masivo de datos en las relaciones laborales. ¿Herramienta de "objetivización"?

A través del tratamiento masivo de datos en el ámbito de la empresa es más posible la vulneración de los derechos fundamentales del trabajador (derecho a la protección de datos y derecho a la intimidad) que en el simple tratamiento diario de dichos datos en los diferentes estadios de la relación laboral. Si, en general, el tratamiento de los datos del trabajador en este ámbito viene amparado por el propio contrato laboral, sin que sea preciso el consentimiento del interesado, obviamente con la finalidad propia de la actividad laboral, en el caso del tratamiento masivo debe aplicarse un cuidado especial en mantener dicho tratamiento en este contexto. En todo caso, aunque la empresa no se encuadre en la relación de actividades que precisan de un delegado de protección de datos, se recomienda su contratación cuando se desarrolla este tipo de tratamientos de forma continua.

Si se busca el análisis del funcionamiento de la plantilla con el objeto de maximizar la productividad de los trabajadores, se justifica perfectamente esta actuación sobre los datos y no es preciso solicitar el consentimiento de la plantilla. No obstante, no hay que olvidar cumplir el derecho a la información de los empleados sobre dicho tratamiento masivo. En cualquier caso, siempre hay que buscar el equilibrio entre el poder de dirección y los derechos fundamentales de los trabajadores.

El tratamiento masivo de datos puede ser una herramienta adecuada para la gestión de la plantilla, en concreto, para la evaluación de su rendimiento a través del análisis de la información extraía por capas y con una visualización sencilla sobre los resultados que sirva para tomar decisiones sobre los cambios precisos en los distintos departamentos de la empresa, no solo con el fin de ahorrar costes, sino también de valorar la capacidad y talento de los trabajadores. Además, su utilización tiene otro efecto positivo: ahorra tiempo y esfuerzo en la gestión.

¿Qué buenas prácticas serían recomendables en el establecimiento de un sistema de control de la actividad laboral? (Artículos 89 y 90 del Proyecto LOPD)

Es recomendable el desarrollo de políticas corporativas bien definidas y claras que se actualicen cada cierto tiempo (de acuerdo con la evolución de los riesgos en relación con el avance de las tecnologías) y de las que se informe debidamente a toda la plantilla.

Así, la política de la empresa debe ser especialmente clara y cuidadosa en las medidas que aplicará en el control del correo electrónico, acceso a Internet, así como sobre los archivos que deben mantenerse en los ordenadores u en otros medios de almacenaje, cuyo propietario es la empresa. Es adecuado crear manuales de utilización que clarifiquen los principales interrogantes sobre su uso y sobre el control empresarial que se puede ejercer sobre ellos.

Es fundamental delimitar los usos privados de los laborales de los instrumentos puestos a disposición del trabajador tales como los ordenadores, tabletas o móviles. Dichos medios de trabajo ya no se sitúan solo en el centro de la actividad laboral, sino que se pueden trasladar a otros espacios privados, complicando aún más la delimitación de la vida privada y laboral. Se recomienda que se circunscriba el uso de los medios informáticos y de comunicación para actividades laborales, restringiendo la utilización privada de dichos instrumentos. Una vez decidida esta política, es necesario informar claramente a los trabajadores a los efectos de eliminar toda expectativa de intimidad en la utilización de los medios.

No obstante, si se decide el uso mixto, una de las prácticas más adecuadas es reconocer espacios privados, donde el trabajador puede almacenar sus datos personales, al margen de la relación laboral, y así pueda preservar su vida personal, sin que la empresa pueda entrar a controlar este contenido específico. Con este fin es necesario identificar estos espacios por ambas partes.

En todo caso, siempre se precisa la actualización continua de las medidas establecidas en la política de control informático y de las comunicaciones, al menos, se recomienda una vez al año. Deben ser acciones dinámicas, que se revisen periódicamente con el fin de incluir nuevas finalidades o tratamientos, especialmente teniendo en cuenta la evolución de las tecnologías.

Existen otros mecanismos que pueden ser útiles en este contexto como la inclusión de filtros de acceso a ciertas páginas web, la criba de los destinatarios o de los contenidos de los correos electrónicos, el aviso diario informativo sobre el uso y sus límites cada vez que el trabajador enciende el ordenador o la tableta o cuando empieza a utilizar el correo electrónico, entre otros.

¿Existen las condiciones adecuadas para que el Big Data permita una mejora sustancial de las herramientas de prevención de riesgos laborales y de vigilancia de la salud?

En este ámbito, hay que ser especialmente cuidadosos, dado que se trata de datos especialmente protegidos en este ámbito. Así, el empresario no puede acceder a este tipo de datos personales de sus trabajadores, sin su consentimiento expreso, a excepción de los supuestos en el que el contexto exija ese conocimiento con el fin de eliminar riesgos laborales. E incluso hay que poner de manifiesto que dicho consentimiento es complicado de justificar como licito, dado que en el contexto de la relación laboral es difícil valorar la libertad de ofrecerlo, dado que se solicita por la

empresa en el especial ámbito de una relación que no es de igualdad entre las partes, con lo cual es fácil entender dicho consentimiento como viciado.

Salvados dichos inconvenientes, otra cuestión es su utilidad. Se entiende que estas herramientas pueden ser adecuadas para el análisis de los datos desde un punto de vista desagregado, por ejemplo, desde la perspectiva de género o de edad. La aportación de un examen disgregado puede ayudar a la empresa a aplicar medidas en materia de prevención de riesgos más adecuadas al perfil del trabajador.

¿Qué limitaciones tiene el uso de datos biométricos en el entorno laboral? (huella dactilar, iris, etc.)

Estos datos personales se califican dentro del concepto de categorías especiales por el RGPD, cuyo tratamiento, en principio, precisaría de un consentimiento expreso, incluso en este ámbito laboral. En este contexto, se entiende por datos biométricos, aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

El Consejo de Ministros de la UE en el documento "*Recommendation CM/Rec (2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment"* (2015) ha recomendado que el control biométrico solo se emplee cuando es necesario para proteger el legítimo interés del empresario, trabajadores o terceros, y siempre que no haya otros medios de control menos intrusivos y se apliquen medidas de seguridad adecuadas y estrictas. Es decir, su uso debe ser subsidiario. En todo caso, solo puede basarse en métodos científicos de reconocimiento.

Entrando en el análisis de los distintos datos biométricos. El propio RGPD señala que el tratamiento de fotografías debe considerarse como un tipo de dato biométrico, pero, únicamente quedarán incluidas en dicha definición, las fotos que son tratadas con medios técnicos específicos con el fin de que permitan la identificación de una persona física. En todo caso, se ha admitido por la AEPD como lícita la identificación mediante fotografías anexadas a tarjetas de identificación del trabajador, cuando esta sea la única forma de identificarse por razones de seguridad, sin necesidad de consentimiento por parte del trabajador, basada en la finalidad de seguridad. Asimismo, hay sentencias que han aceptado el uso por la empresa de las fotos de los trabajadores, que han sido colgadas por ellos en las redes sociales, a las que se puede acceder sin necesidad de utilizar clave ni contraseña alguna y que, además, aparecen tomadas en un lugar público.

Otros ejemplos de datos biométricos son las huellas digitales, el iris del ojo, patrones faciales, o la voz, que han sustituido el sistema de control de entrada y salida tradicional de fichaje estos, que

son más precisos y, además, evitan fraudes en el control. Pero ¿es lícito el tratamiento de estos datos a través de estos medios en el ámbito del contrato de trabajo, sin necesidad de consentimiento del trabajador? A favor se ha manifestado la AEPD en 1999 en relación con la licitud, sin necesidad de consentimiento, del tratamiento de los datos obtenidos por la huella digital de los empleados públicos en la Administración Pública. Posteriormente, en 2007 volvió a pronunciarse sobre la información obtenida a través de la huella digital, señalando que no contiene ninguna información sobre la personalidad del trabajador, siendo su trascendencia similar a la de un número personal. Por lo que, incluso se podría concluir que ni siquiera es un dato personal. Por otra parte, el Tribunal Supremo ha declarado, en relación con la lectura biométrica de la mano de los trabajadores para controlar su asistencia al trabajo, que este medio no lesionaba los derechos fundamentales de los trabajadores, en concreto, el de intimidad, sobre todo porque se trata de un sistema inocuo para la salud. Con lo cual, valoraba que estos sistemas no vulneraban derechos fundamentales de los empleados.

En este marco, ahora el artículo 9 del RGPD señala que los datos biométricos están catalogados como de categorías especiales y, por tanto, su tratamiento en la empresa no puede hacerse de forma lícita de acuerdo con el propio desarrollo del contrato de trabajo. Con lo cual parece que habrá que obtener el permiso del trabajador afectado y siempre para una finalidad concreta, en este caso, el registro de la jornada laboral.

Sin embargo, en este mismo precepto se establecen excepciones, en las que no es preciso el consentimiento. El RGPD admite que los Estados miembros veten el tratamiento o que incluyan algún tipo de cautela al respecto en relación con los datos analizados, no obstante, por el momento el proyecto de LOPD de noviembre 2018 no señala nada. Teniendo en cuenta que hasta ahora se ha admitido esta práctica como parte del control empresarial con el fin de facilitar la organización de la actividad laboral, es posible que su consideración no varié. Una segunda posible excepción es que se entiende que es lícito el tratamiento cuando es necesario para el cumplimiento de las obligaciones y ejercicios de los derechos específicos del responsable del tratamiento, en este caso, la empresa. Si se estima, tal y como parecer haberse hecho desde la AEPD y los tribunales, que es un medio adecuado a las necesidades del control empresarial. Desde esta idea, asimismo sería lícito este tratamiento, sin necesidad del consentimiento de los trabajadores.

Lo que suscita más dudas es la recomendación hecha desde el Consejo de Ministros de la UE de utilizar estos medios de forma restrictiva, cuando no se pueden emplear otros. Obviamente siempre es posible volver a sistemas más tradicionales a través del control mediante ficha o firma, aunque sean menos eficiente. Lo cual se entiende que habrá que interpretar con lógica está restricción, utilizando estos medios siempre que no sean especialmente invasivos, y no se vulneren los derechos fundamentales de los trabajadores implicados.