Nyon 191217

Principales 10 principios para la protección y la privacidad de los datos de los trabajadores

Introducción

Aunque los datos, los big data y los conjuntos de datos son utilizados en medida cada vez mayor por las empresas para informar sobre decisiones administrativas, apenas existen normas de protección de los datos y la privacidad de los trabajadores. Este documento proporciona 10 principios operativos que abordan este desequilibrio. Al ofrecer reivindicaciones concretas con respecto a la recopilación y el uso de datos empresariales, estos principios habilitarán a los trabajadores y garantizarán un uso ético y sostenible de los datos. Definitivamente hay que actuar ahora. Se requiere acción para salvaguardar los intereses de los trabajadores y mantener un sano equilibrio de poder en los lugares de trabajo. Los 10 principios provistos en este documento han sido desarrollados por UNI Global Union a tal fin.

Los datos se les ha denominado el nuevo oro. Se comercializan, analizan y utilizan en marketing, publicidad y gestión de recursos humanos. También es el componente básico de la inteligencia artificial y los algoritmos. Para 2030, se estima que entre el 15% y el 20% del PIB mundial combinado se basará en flujos de datos. También son el cimiento de innumerables empresas y servicios nuevos que individualizan cada vez más muchos aspectos de nuestra economía y de nuestra sociedad, a saber, las plataformas de la llamada economía de los bolos.

Como ciudadanos, dejamos a diario un reguero de datos: de lo que buscamos en Google, a las aplicaciones en nuestros teléfonos móviles, de trayectos en taxis, pisos que alquilamos, de lo que compramos, a nuestras tarjetas de fidelización, nuestros registros de salud, llamadas telefónicas a servicios al cliente. Sin mencionar los lugares que visitamos, los correos electrónicos que enviamos, los amigos de Facebook que tenemos y los tuits que escribimos. Hacer todo esto proporciona a las empresas datos: sobre nosotros y nuestra red de amigos. Los datos son simplemente el regalo más grande que no nos damos cuenta de que estamos haciendo.

También proporcionamos datos como trabajadores: nuestros CV, nuestros datos biométricos, como nuestras huellas dactilares o escáneres de iris, y los abundantes datos que se nos extraen cuando los empleadores supervisan nuestros flujos de trabajo. Los datos, o más bien los conjuntos de datos de dentro y fuera de la empresa, también son utilizados por la dirección en las decisiones en materia de recursos humanos. ¿Quién es contratado? ¿Quién es ascendido? ¿Debería ser alguien despedido o advertido? ¿Son los trabajadores productivos hoy y, de no ser así, por qué no lo son? La aplicación y el uso en las empresas incluso ha provocado la pregunta de si los datos están sacando al humano de los recursos humanos.

¿Pero, en realidad, quién posee los datos que proporcionamos? ¿Y qué datos existen 'allá afuera' sobre usted y sobre mi? Estas dos preguntas son difíciles de responder. El CEO de LinkedIn ha dicho que la gran mayoría de los datos del mundo está finalmente en manos de Big Tech: Google, Facebook, Amazon, Microsoft y Apple. Un feed de Twitter reciente afirmaba que por 1000 USD puede obtener de una empresa que le proporcione toda la información posible sobre una persona. Sabemos que ciertas compañías son expertas en extraer datos y venderlos a otros para que puedan manipular nuestros puntos de vista. Al orientarnos con historias particulares y pagando cuentas

falsas de Twitter y Facebook para difundir opiniones, ahora sabemos que tanto los resultados de las elecciones en Estados Unidos como los del Brexit fueron influenciados y manipulados utilizando datos.

En Japón, el gobierno se está preparando para lanzar los denominados bancos de datos. Oficinas públicas que ayudarán a los ciudadanos a decidir qué datos quieren poner a disposición. En Estonia, un país con uno de los sistemas de gobierno electrónico y uso de datos más completos del mundo, los datos de los ciudadanos están sujetos a principios legales rigurosos que facultan a la persona individual para decidir qué datos están disponibles y cómo pueden utilizarse. Sin embargo, muchos países se están quedando atrás en lo que respecta a proporcionar a los ciudadanos una forma clara y transparente de saber qué información existe, y sobre todo en lo que respecta a proporcionar a los ciudadanos los medios para controlarla.

Aunque leyes en materia de privacidad y protección de datos existen bajo varias formas en muchos países, los datos derivados de monitorear a los trabajadores no están específicamente cubiertos por estas leyes. UNI Global Union está cooperando con la organización global IEEE para crear una norma global para la gobernanza transparente del empleador de los datos de los empleados. También es esencial que los sindicatos busquen implementar, a través de acuerdos colectivos de empresas y/o sectoriales, derechos de los trabajadores sobre los datos y disposiciones de protección. Sin dichas disposiciones, el equilibrio de poder en las empresas quedará para siempre en manos de decisiones administrativas unilaterales basadas en datos. Dada la relativa facilidad de combinar datos de muchas fuentes, sin tener voz ni influencia sobre qué datos se usan y cómo, los trabajadores estarán extremadamente desfavorecidos. De hecho, se puede afirmar que la protección y la privacidad de los datos de los trabajadores es la próxima meta para los sindicatos a medida que la economía digital va tomando forma.

Dada la importancia de los datos del lugar de trabajo, UNI Global Union exige que: **Los trabajadores y sus representantes sindicales deben tener el derecho de acceder a los datos que se recogen sobre ellos y a través de sus procesos de trabajo, influenciarlos, modificarlos y suprimirlos .**

Este documento plasma esta reivindicación clave y la divide en 10 puntos de acción específicos.

Índice

1 Los trabajadores deben tener acceso a los datos recopilados sobre ellos y ejercer influencia sobre ellos

Los trabajadores deben tener el derecho de acceso a los datos recopilados sobre ellos, incluido el derecho a que los datos sean modificados, bloqueados o suprimidos.

Esto incluye:

a) El consentimiento no puede ni debe ser el fundamento jurídico del tratamiento de datos en el trabajo.
b) El trabajador debe poder obtener, previa solicitud, a intervalos razonables y sin demora excesiva, la confirmación del tratamiento de los datos personales que le conciernen. La comunicación debe estar en una forma inteligible, incluir toda la información sobre el origen de los datos, así como cualquier otra información que el controlador debe proporcionar para garantizar la transparencia del procesamiento.
c) Un trabajador debe tener derecho a la portabilidad de los datos, es decir, el derecho a desplazar, por ejemplo sistemas de clasificación y categorización de una plataforma a otra.
d) De conformidad con la legislación y la práctica nacionales, o con los términos de los convenios colectivos, los datos personales podrán ser comunicados a los representantes del trabajador, pero sólo en la medida en que dichos datos sean necesarios para representar adecuadamente los intereses del trabajador o si dichos datos son necesarios para el cumplimiento y supervisión de las obligaciones establecidas en los convenios colectivos.

2 Aplicación de salvaguardias sostenibles de tratamiento de datos

Para todas las formas de tratamiento de datos, los empleadores deben garantizar el respeto de las siguientes salvaguardias. En particular:

a) informar a los trabajadores de manera clara y completa antes de la introducción de sistemas y tecnologías de información que permitan el seguimiento de sus actividades. La información facilitada debe mantenerse actualizada y debe tenerse en cuenta el principio 3 abajo. La información debe incluir el propósito de la operación, el período de conservación o de respaldo, así como la existencia de los derechos de acceso y rectificación de los trabajadores y cómo pueden ejercerse estos derechos. Esta salvaguardia incluye cuando cambian los propósitos y sistemas de monitoreo
b) adoptar las medidas internas apropiadas relativas al tratamiento de dichos datos y notificar a los trabajadores con antelación, lo que incluye la realización de una evaluación del impacto sobre la privacidad cuando las tecnologías pueden dar lugar a un alto riesgo para las personas, (véase el principio 5 abajo)
c) consultar a los trabajadores en circunstancias en que se sospeche la existencia de una vulneración del derecho de los trabajadores al respeto de la vida privada y de la dignidad humana. Respetar en dichos casos el derecho de los trabajadores a solicitar el veto de dicho monitoreo de datos hasta que el empleador pueda probar por escrito y posteriormente recibir la aprobación de los trabajadores de que se respeta plenamente el derecho de los empleados al respeto de la vida privada y la dignidad humana (véase el principio 5)

3 Debe aplicarse el principio de minimización de los datos

El principio es que los empleadores solamente pueden:

> "Recopilar datos y sólo los datos correctos para los propósitos correctos y sólo los propósitos correctos, para ser utilizados por las personas adecuadas y sólo las personas adecuadas y por la cantidad adecuada de tiempo y sólo la cantidad adecuada de tiempo".

Los empleadores deben adoptar medidas adecuadas para garantizar que respetan en la práctica los principios y obligaciones relativos al tratamiento de datos con fines laborales. Esto incluye los principios de proporcionalidad y subsidiariedad: que la recopilación de datos debe limitarse a lo necesario para alcanzar los objetivos de recopilación en cuestión, es decir, que el contenido y la forma de la acción deben estar en consonancia con el objetivo perseguido.

A petición de la autoridad supervisora, los empleadores deben poder demostrar su conformidad con dichos principios y obligaciones. Estas medidas deben adaptarse al volumen y la naturaleza de los datos tratados, al tipo de actividades que se están llevando a cabo y también deben tener en cuenta las posibles consecuencias para los derechos y libertades fundamentales de los trabajadores.

4 El tratamiento de datos debe ser transparente

a) La información relativa a los datos de carácter personal de los empleadores deberá ponerse a disposición del interesado directamente o por intermedio de sus representantes o llevarse a su conocimiento por otros medios apropiados.
b) Los empleadores deben proporcionar a los trabajadores la información siguiente:
    i. las categorías de datos personales a tratar y una descripción de los fines del procesamiento;
    ii. los destinatarios o las categorías de destinatarios de los datos personal;
    iii. los medios que los trabajadores tienen para ejercer los derechos establecidos en el principio 1, sin perjuicio de los más favorables previstos por la legislación nacional o en su sistema jurídico;
    iv. cualquier otra información necesaria para garantizar un tratamiento justo y lícito.
c) Debe facilitarse una descripción particularmente clara y completa de las categorías de datos personales que pueden recopilar las TIC, incluida la videovigilancia y su posible utilización.
d) La información debe proporcionarse en un formato accesible y mantenerse actualizada. En cualquier caso, dicha información debe proporcionarse antes de que el empleado lleve a cabo la actividad o acción en cuestión y se facilite a través de los sistemas de información utilizados normalmente por el empleado.

5 Las leyes sobre la intimidad y los derechos fundamentales deben respetarse en toda la empresa

Esto incluye el respeto de todos los convenios mundiales y regionales sobre derechos humanos,[1] incluyendo:

- La Declaración Universal de Derechos Humanos de la ONU
- El Código de prácticas de la Oficina Internacional del Trabajo de 1997 sobre la protección de los datos personales de los trabajadores,

El empleador también debe:

a) respetar la dignidad humana, la intimidad y la protección de los datos personales en el tratamiento de datos personales con fines de empleo, en particular para permitir el libre desarrollo de la personalidad del trabajador, así como las posibilidades de relaciones individuales y sociales en el lugar de trabajo
b) La comunicación debe ser lícita y no incluir declaraciones difamatorias
c) Las instalaciones de comunicaciones empresariales no deben ser utilizadas como un medio de acoso sexual, ni para difundir comentarios ofensivos con el fin de discriminar.

El empleador puede exigir un descargo de responsabilidad cuando los trabajadores se comunican internamente y externamente en el sentido de que las opiniones expresadas son sólo del autor y no de la empresa.

[1] http://www.ohchr.org/Documents/Publications/CoreTreatiesen.pdf

6 Los trabajadores deben tener pleno derecho a la explicación cuando se usan los datos

Este principio se refiere a las decisiones tomadas por la dirección que incluyen la obtención de datos desde dentro y fuera de la empresa. Por ejemplo, en los procesos internos y externos de contratación, los trabajadores deben tener el derecho de saber sobre qué base se ha tomado una decisión. Esto es para proteger a los trabajadores contra las decisiones discriminatorias basadas en predicciones de datos, no menos en cuanto a la salud.

El empleado debe ser informado cuando se toman decisiones importantes basadas en datos internos y externos.

7 Los datos biométricos y la información de identificación personal (PII) deben estar protegidos

La recopilación y el tratamiento ulterior de los datos biométricos sólo deben llevarse a cabo si no hay otros medios menos intrusivos disponibles y sólo si van acompañados de salvaguardias adecuadas, incluidas las salvaguardias adicionales previstas en el principio 2.

El procesamiento de datos biométricos y otras PII debe basarse en métodos científicamente reconocidos y debe estar sujeto a los requisitos de estricta seguridad y proporcionalidad.

8 Equipos que localizan a los trabajadores

El equipo que localiza a los trabajadores sólo debe introducirse si resulta necesario para lograr el objetivo legítimo perseguido por los empleadores y su uso no debe conducir a un seguimiento continuo de los trabajadores. En particular, el monitoreo no debe ser el propósito, sino sólo una consecuencia indirecta de una acción necesaria para proteger la producción, la salud y la seguridad o para asegurar el funcionamiento eficiente de una organización. Habida cuenta del potencial de vulnerar los derechos y libertades de las personas afectadas por el uso de estos dispositivos, los empleadores deben garantizar todas las salvaguardias necesarias para el derecho de los trabajadores a la intimidad y a la protección de los datos personales, incluidas las salvaguardias previstas en el principio 2.

De conformidad con el principio 3 sobre la minimización de datos, los empleadores deben prestar especial atención a la finalidad para la que se utilizan dichos dispositivos. Los empleadores deberían aplicar procedimientos internos apropiados relacionados con el tratamiento de estos datos y notificar previamente a las personas interesadas.

9 Debe establecerse un organismo multidisciplinario de gestión de datos entre empresas

Debe establecerse un órgano multidisciplinario de gestión de datos entre empresas para regular la formación de datos, el almacenamiento, la manipulación y las cuestiones de seguridad. Esto incluye disposiciones en las que todos los representantes del organismo, incluidos los delegados sindicales, reciben capacitación adecuada en materia de datos para estar preparados para trabajar con las empresas en la defensa y la retención de una política sostenible de protección de datos.

10 Todo lo anterior debe ser implementado en un convenio colectivo

Los principios anteriores deben aplicarse y hacerse cumplir mediante la negociación colectiva sectorial o empresarial. En ausencia de dicha negociación, el empleador debería establecer un órgano de gobierno de conformidad con el principio 9.

Fuentes:

Este documento se ha inspirado y obtenido información de los siguientes documentos clave

1) GDPR (http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf)

2) Recomendación CM/Rec(2015) del Consejo de Europa(2015) del Comité de Ministros a los Estados Miembros sobre el tratamiento de datos en el marco del empleo https://www.apda.ad/system/files/cm-rec-2015-5-en.pdf

3) (2017): GRUPO DE TRABAJO "ARTÍCULO 29" SOBRE LA PROTECCIÓN DE LOS DATOS, Opinión 2/2017 sobre el tratamiento de datos en el trabajo http://ec.europa.eu/newsroom/document.cfm?doc_id=45631