Organización Internacional del Trabajo

Nota informativa de la OIT

Mejorando el derecho a la protección de datos de los trabajadores

Introducción

Este informe discute cómo la extracción de datos de nuestra vida privada y laboral puede influenciar nuestras oportunidades de trabajo, el equilibrio de poderes entre la dirección y el trabajo, además del derecho que los trabajadores deberían tener sobre estos datos para prevenir un estrechamiento de sus oportunidades en el mercado laboral.

Todo lo que es digital extrae y/o produce datos. Desde el uso de las redes sociales, la información de pago con una tarjeta de crédito, los hábitos de consumo, cuáles sitios o aplicaciones se usan y cuándo, hasta los 14 sensores en los smartphones que extraen datos sobre localización, sonido y temperatura alrededor, velocidad y mucho más. Todos estos datos son usados para inferir cosas sobre nosotros – como ciudadanos y como trabajadores. A fin de categorizarnos y hacer predicciones sobre nosotros para publicidad, pero también para la manipulación del pensamiento, la disponibilidad de trabajo para algún individuo y, en última instancia, para definir cuán inclusivo y diverso es el mercado de trabajo.

Es importante notar que no solamente su vida y carrera son afectadas por esta extracción de datos. A medida que los datos se acumulan, son usados para comparar personas o grupos de personas en infinitas otras categorías. Por ejemplo, la calificación de clientes con relación a características de trabajo, tipos de amistades con potencial de sindicalización. El índice de masa corporal con la velocidad de trabajo. Acento, código postal y percepción sobre confiabilidad. Los sistemas de algoritmos usados para encontrar todas esas correlaciones, probabilidades, predicciones y diferencias se hacen cada vez más elaborados a medida que la cantidad de datos crece exponencialmente. Lo que uno hace, en otras palabras, afecta sin que uno sepa la vida de otros.

Datos en el trabajo

Exacerbada por la pandemia de COVID-19, la tendencia hacia los espacios laborales guiados digitalmente solamente ha crecido. Todos los servicios y sistemas digitales en los espacios de trabajo extraen datos de los trabajadores. Podemos identificar 5 formas en las que esto ocurre:

Data at work

Recolección directa:
de candidatos, empleados, clientes

Perfiles/Conjuntos de datos comprados
de terceros

Extracción de rastros de datos
de sistemas de computadores y redes

Datos derivados de sensores
por aparatos manuales, vestimentas, o equipos

Datos audiovisuales
de CCTV, llamadas telefónicas, reconocimiento facial

- **Recolección directa:** Su CV contiene mucha información valiosa. Desde sus empleadores anteriores, hasta su formación, tal vez hasta sus intereses en el tiempo libre y otras actividades. Los empleadores pueden también recolectar datos directamente de sus clientes (qué compran, con qué frecuencia, qué bienes o servicios les interesan en sitios etc.) o de sus actuales empleados (por ejemplo, cuán frecuentemente se enferman, cuántas horas o turnos trabajan etc.).
- **Perfiles de datos comprados:** Existen distintos así llamados "data brokers" (corredores de datos) en el mundo cuyo modelo de negocios está integralmente basado en la compra, compilación y venta de conjuntos de datos. Estos pueden ser conjuntos de datos de tráfico agregados, o datos sobre la "confiabilidad" de ciertos grupos de personas, o perfiles sobre calificación crediticia, nivel de salud o educación ordenados geográficamente o por estatus socioeconómico.
- **Extracción de rastros de datos:** Cuando inicia sesión en su email o servidor del trabajo deja un rastro de sus actividades. ¿A qué hora inició la sesión, a qué documentos accedió? Algunos sistemas, como el Office365, crean reportes sobre cuán "productivo" se ha sido, cuánto tiempo de "concentración" ha tenido etc. Vale preguntarse si la dirección tiene acceso a este tipo de medios también.
- **Datos derivados de sensores:** Algunas oficinas tienen sensores a lo largo del edificio: Debajo de las mesas para registrar cuánto se usó y cuánto estuvo vacía. En puertas para registrar cuánto se usó una sala, o no. Algunos trabajadores tienen que usar escáneres manuales o vestimentas como un Fitbit o aparatos para localización. Todos estos dispositivos producen datos que pueden y son usados por la dirección.
- **Datos audiovisuales:** Otros tipos de datos son derivados de sistemas audiovisuales. Los tonos de voz y lo que dicen los trabajadores de centros de llamadas son medidos y evaluados. Escucha de llamadas con teléfonos móviles. CCTV o reconocimiento facial son usados para localizar y identificar trabajadores. Aunque son fuertemente criticados, algunos de esos sistemas se usan para predecir el estado emocional de los trabajadores: ¿Están cansados? ¿Parecen tristes, frustrados, felices o nerviosos?

Independientemente de los medios de extracción, los sistemas de vigilancia y supervisión digitales juntan datos sobre los trabajadores y sus acciones y no acciones. Aunque la vigilancia no es algo nuevo, la naturaleza digital de los sistemas actuales tiene características particulares que influenciarán la forma como los sindicatos se deberían relacionar con ellos. Imagine un sistema que monitorea la productividad de los trabajadores de un piso de una fábrica por medio de cámaras de vigilancia y sensores manuales. Primeramente, el sistema es imposible de evitar, considerando que está acoplado al proceso y a los aparatos de trabajo. En segundo lugar, la vigilancia es comprensiva – recolecta una gran cantidad de datos de fuentes diversas. En tercer lugar, la dirección recibe información instantáneamente cuando los datos son colectados en tiempo real. En cuarto lugar, el sistema es interactivo, ofreciendo comunicación y comentarios en tiempo real – en nuestro caso por pantallas en la fábrica que muestran el desempeño de cada trabajador.

Los empleadores pueden usar estos datos para medir la productividad y eficiencia de cada trabajador (como sea que se definan esas características). Pueden evaluar cálculos sobre la probabilidad de que usted, por ejemplo, alcance sus metas, sea apreciado por los clientes, trabaje rápidamente, o se dedique al trabajo. O pueden usarlo para hacer predicciones: ¿Cuál es la probabilidad de que deje la empresa luego, se enferme, se haga más lento, o se una a un sindicato?

El exacto uso de los datos por parte de los empleadores depende del propósito de los sistemas que instalen y los análisis de datos que conduzcan. En algunos casos, los trabajadores pueden aceptar la extracción de datos. Por ejemplo, los trabajadores pueden apoyar la extracción de datos con propósitos de salud y seguridad para evitar accidentes o medir el tiempo de trabajo y evitar el estrés o burnout. Lo que importa es que los trabajadores sepan y tengan influencia sobre si la extracción de datos debería ocurrir, cuáles son los propósitos de la extracción, cómo se usan los datos, y qué pasa con los datos después. El informe 2 discute los daños e impactos de los algoritmos ya vividos por los trabajadores.

La economía política de la extracción de datos

Aunque trabajadores y empleadores en principio puedan consentir los propósitos de la extracción y análisis de los datos, una cuestión mayor entra en juego. ¿Concretamente, queremos de hecho que se cuantifiquen nuestras acciones, transformando nuestro trabajo en puntos de datos que pueden o no ser usados indebidamente? ¿Si los trabajadores y trabajadoras son percibidos más como números o puntos en una norma estadística que como humanos, cómo esto afectará los derechos humanos y laborales?

Una narrativa común es que los datos son "el nuevo petróleo" – un recurso extraído que es valioso, pero si no es refinado no puede realmente ser usado. Por lo tanto, los datos tienen que ser analizados y compilados. Tienen que transformarse en un bien que pueda ser reusado para añadir valor a las cadenas de producción y servicio. Esta narrativa entonces afirma que los datos son un commodity que puede ser comprado y vendido. Siguiendo esa afirmación, los datos de los trabajadores pueden ser monetizados. Sin embargo, considerando la contribución de los trabajadores a este medio de producción en términos monetarios, demandando una redistribución de el valor añadido de vuelta a los trabajadores, solo se solidifica y tal vez hasta justifica la mercantilización del trabajo.

Críticos de esta perspectiva económica sobre los datos afirman que los datos deben ser vistos en una perspectiva de derecho y poder. Los que recolectan los datos son los que ganan poder sobre mercados, competidores, ciudadanos y trabajadores. Solamente sus análisis, sus historias dominan y terminan manipulando qué servicios, puntos de vista, productos nos son revelados individualmente, sin considerar los derechos humanos y otros aspectos morales.

La aclamada autora de La Era del Capitalismo de Vigilancia, Shoshana Zuboff, afirma firmemente que deberíamos considerar ilegales lo que ella llama "mercados de comportamiento futuro"[1]. Se refiere con esto al intercambio de inferencias sobre datos que son usados para constantemente manipularnos sin que nos demos cuenta. Como lo describe, los recolectores de datos necesitan una cantidad enorme de datos para ofrecer certeza a los clientes, al igual que una variedad de datos para asegurar que sus predicciones y modelos sean lo más precisos posibles. Esto lleva a economías de alcance y escala – y por ende a la concentración del poder en manos de pocos, compañías mundiales muy ricas: Google, Meta, Apple, Amazon, Microsoft, Alibaba y Tencent.

Mientras la extracción de datos desde una perspectiva económica es solo restringida por la ley (por ejemplo, regulaciones de protección de datos), un abordaje basado en derechos estipula que los datos solamente pueden ser extraídos si respetan un conjunto amplio de derechos.

La ACNUDH publicó en 2018[2] una nota guía sobre los principios del abordaje basado en los derechos humanos para datos. Recomendaban allí seis principios, cada uno con subprincipios:

1. **Participación**: Participación de grupos relevantes de la población en los ejercicios de extracción de datos, incluyendo planeamiento, recolección y análisis de datos.
2. **Desglose de datos**: El desglose de datos permite que los usuarios de los datos comparen grupos poblacionales, y que entiendan la situación de grupos específicos. El desglose requiere que datos sobre características relevantes son recolectados.
3. **Identificación propia**: Con el propósito de recolección de datos, las poblaciones interesadas deberían ser definidas por sí mismas. Los individuos deberían tener la opción de revelar, o retener, información sobre sus características personales.
4. **Transparencia**: Los recolectores de datos deberían proveer información clara y accesible abiertamente sobre sus operaciones, incluyendo diseño de pesquisa y metodología de recolección de datos. Los datos recolectados por agencias del Estado deberían estar abiertos para el público.
5. **Privacidad**: Los datos recogidos por recolectores de datos deben mantenerse protegidos y privados, y la confidencialidad del comportamiento de los individuos y de sus datos personales debe mantenerse.
6. **Responsabilidad**: Los recolectores de datos son responsables por el respeto a los derechos humanos en sus operaciones, y los datos deben ser usados para responsabilizar al Estado y otros actores por la protección de los derechos humanos.

Para los trabajadores estos principios significarían que ellos tienen el derecho de participar de la decisión sobre cuáles datos serán extraídos, para qué propósitos serán usados, verificar que los datos sean representativos y por lo tanto no discriminatorios y con los derechos humanos respetados durante todo el proceso. ¿Estos derechos están garantizados para los trabajadores en las regulaciones de protección de datos en todo el mundo?

1 https://www.project-syndicate.org/onpoint/surveillance-capitalism-exploiting-behavioral-data-by-shoshana-zuboff-2020-01?barrier=accesspaylog
2 https://www.ohchr.org/documents/issues/hrindicators/guidancenoteonapproachtodata.pdf
3 https://techgdpr.com/blog/difference-between-pii-and-personal-data/
4 https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Regulación de protección de datos y trabajadores

Las regulaciones de protección de datos alrededor del mundo se centran en el procesamiento de los datos personales, o adicionalmente, información identificada personalmente.[3] Según la UNCTAD, el 19% de todos los países del mundo no tiene regulaciones de protección de datos en vigor.[4] Con relación a los datos de los trabajadores específicamente, las regulaciones de protección de datos en el resto del mundo pueden ser divididas en tres categorías. Las que incluyen artículos específicos sobre datos de los trabajadores (como el Reglamento General de Protección de Datos de la Unión Europea – el GDPR), los que lo hacen implícitamente como en los países de África, Latinoamérica y Asia-Pacífico, y los que explícitamente excluyen a los trabajadores (como el Acta de Privacidad del Consumidor de California en 2018 – el CCPA y parcialmente el Acta de Privacidad Australiana de 1988[5]).

La mayor parte de las regulaciones se encuentra en la segunda categoría,[6] en la que todos los requerimientos legales relacionados con la privacidad de datos se aplican a la recolección, procesamiento, transferencia y uso de datos de empleados. Además, la mayoría cuenta con el "consenso informado"[7] para la extracción y uso de los datos de los trabajadores por parte del empleador. Esto es contrario a el GDPR europeo que explícitamente dice que, debido al desequilibrio de poder entre trabajador y dirección, los trabajadores nunca serán enteramente libres para ofrecer su consenso. Con pocas excepciones,[8] el consenso informado es, por lo tanto, una base ilegal de procesamiento de datos de trabajadores en la GDPR.

La tercera categoría, que explícitamente excluye a los trabajadores, no es muy común, sin embargo, varios proyectos de ley sobre protección de datos están actualmente bajo negociación en los EE. UU. y buscan excluir a los trabajadores de cierta manera. La CPPA fue enmendada por el proyecto de ley de la asamblea 25 (AB-25) en 2019, que retiró la obligación de los empleadores hacia los residentes de California en posiciones de solicitantes de empleo, empleados, personas contratistas autónomas, oficiales corporativos y ejecutivos.[9] Independientemente de las excepciones del AB-25, los empleadores siguen obligados a notificar clientes incluyendo miembros de su mano de obra, además de solicitantes de trabajo sobre las categorías de información personal que recolectan y su propósito de uso en o antes del punto de recolección.

En resumen, con excepción de ciertos trabajadores cubiertos por la GDPR, los derechos sobre datos de los trabajadores están mal definidos en las regulaciones de protección de datos alrededor del mundo. Aunque la mayoría de las regulaciones sobre protección de datos implícitamente incluye a los trabajadores, también cuentan en el "consenso informado" como base del procesamiento de los datos personales de los trabajadores.[10] Sin embargo, como está declarado en la GDPR, el consenso informado no puede ser libremente dado por trabajadores en la situación de relaciones de poder entre dirección y trabajadores[11]. Además, aunque los empleadores en la mayoría de las protecciones de datos son obligados a informar a los trabajadores sobre los datos recolectados y el propósito de recolección, los trabajadores no tienen ningún derecho a consulta, revisión, ni de edición o remoción de los datos recolectados.

Ninguna de las regulaciones cumple enteramente con los principios de la ACNUDH, como descritos previamente.

5 https://www.lexology.com/library/detail.aspx?g=0f6d20a7-a6b1-4980-aa0e-a98f1d637d38
6 Ver este libro electrónico para una buena contextualización: https://www.mayerbrown.com/ebooks/A-Global-Guide-to-Employee-Data-Privacy/#/spreads/1
7 La GDPR declara que el consentimiento debe ser "dado libremente, específico, informado y no ambiguo. Eso significa que el portador de los datos debe estar consciente de que está aceptando tener sus datos procesados y no ser forzado a aceptar. Recital 32 - Conditions for Consent - General Data Protection Regulation
8 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-my-employer-require-me-give-my-consent-use-my-personal-data_en
9 https://secureprivacy.ai/blog/ab-25-what-this-ccpa-amendment-means-for-employers-and-employees
10 Ver Artículo 29 de la Guía del Partido de los Trabajadores sobre consentimiento bajo regulación 2016/679, página 7. https://ec.europa.eu/newsroom/article29/redirection/document/51030

Mejorando los derechos de los trabajadores sobre la protección de datos

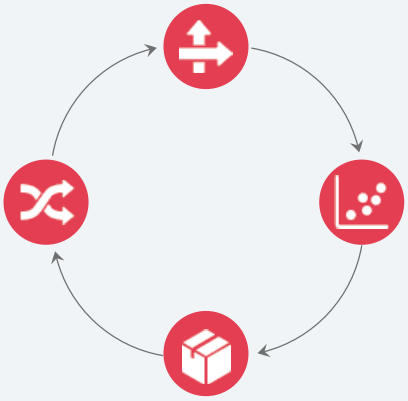
Está claro que los derechos sobre datos individuales y colectivos de los trabajadores están definidos de forma deficiente en la mayoría de los países y regiones. La siguiente gráfica muestra el ciclo de vida de los datos en el trabajo: desde la recolección de datos, el análisis, almacenamiento y descarga, se describen los tópicos que los sindicatos debían tener en cuenta para negociar, al igual que los derechos que los trabajadores deben exigir. Se apoya en la publicación de 1997 de la OIT "Protección de los datos personales de los trabajadores. Un código de practicas de la OIT"[11].

Algunas de las demandas de cada una de las cuatro fases, aunque lejos de ser todas, están cubiertas para trabajadores en la zona del Reglamento General de Protección de Datos de la Unión Europea. Para los trabajadores en la mayoría de las otras jurisdicciones, esos derechos – si negociados – serian nuevos.

Ciclo de Vida de los Datos en el Trabajo

Recolección de datos:
¿Fuentes? ¿Acceso sindical al conocimiento? ¿Derecho a refutar/bloquear?

Descarga de datos:
¿Se venden los datos? ¿A quién? ¿Borrar? ¿Los trabajadores pueden bloquear/negar a quien será vendido? Esto incluye conjuntos de datos, estadísticas, inferencias



Análisis de datos
Usado en productividad y recursos humanos. ¿Cuáles derechos al acceso a los datos, descubrimientos, inferencias tienen los trabajadores? ¿Pueden negar esto? Sindicatos deberían establecer límites para el uso de los datos

Almacenamiento de datos
Servidores - ¿Dónde?¿Quiénes tienen acceso? ¿Bajo qué jurisdicción?
Especialmente importante por las discusiones OMC/comercio electrónico

Recolección de datos

La recolección de datos cubre las herramientas internas y externas de recolección, las fuentes de datos, si los representantes y trabajadores fueron informados sobre las herramientas usadas y si tienen el derecho de negarlas o refutarlas. Mucha extracción de datos es escondida de los trabajadores (o ciudadanos) y los empleadores deben ser responsabilizados.

En el área del GDPR, las compañías son obligadas a conducir evaluaciones de impacto (DPIAs) sobre la introducción de nuevas tecnologías que potencialmente representen un riesgo para la información ajena.

También están obligadas a consultar a los trabajadores.[12] No obstante, muy pocos sindicatos tienen acceso a estas evaluaciones, o ni si quiera saben sobre ellas. Los sindicatos deberían exigir su derecho de participar de esos procesos.

Análisis de datos

En la fase de análisis de datos, los sindicatos tienen que cubrir las brechas regulatorias que fueron identificadas – concretamente la falta de derechos con respeto a la creación de perfiles sobre los trabajadores usando probabilidades estadísticas basadas en los datos

11 https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_112624.pdf
12 Article 35 du RGPD et Avis 2/2107 sur le traitement des données sur le lieu de travail du Groupe de travail «Article 29» sur la protection des données.

recolectados. Pese a que los trabajadores en la zona del GDPR tienen el derecho de saber sobre cuáles inferencias fueron hechas usando sus datos personales directamente, no tienen el derecho de saber a cuáles inferencias están sujetos sin inclusión de sus datos personales.[13] Estas inferencias pueden ser usadas para determinar horarios de trabajo, salarios (si se relacionan a métricas de performance) óptimos o, en recursos humanos, a quién contratar, promover o despedir. Pueden ser usados para predecir comportamientos basados en patrones históricos, datos emocionales y de actividad.

El acceso a las inferencias es clave para el empoderamiento de los trabajadores y ciertamente para los derechos humanos. Los trabajadores deberían tener mayor acceso a esas inferencias y derecho de rectificar, bloquear o hasta borrarlas. Sin estos derechos, habrá poco control sobre el uso de sistemas de algoritmos de los empleadores y los sesgos y discriminaciones basados datos.

En combinación con la fase de recolección de datos, los sindicatos podrían negociar de forma favorable los propósitos de la recolección y análisis de datos. Esto incluye la determinación de límites sobre cuáles usos se pueden dar a los datos colectados y cuáles no.

Almacenamiento de datos

La fase de almacenamiento de datos es importante, sobre todo con relación a acuerdos comerciales y negociaciones sobre flujos de datos. Por ejemplo, las negociaciones de comercio electrónico sobre "datos de flujo libre", dentro y en los márgenes de la Organización Mundial de Comercio, tienen como objetivo eliminar los derechos de cualquier nación de localizar datos adentro del territorio de una nación. Esto puede hacer que los datos sean trasladados a áreas con menos protección de privacidad, lo cual crea un riesgo considerando que los datos de los trabajadores pueden ser vendidos, recompilados, y vendidos de nuevo sin tener que adherir a las políticas de protección de dados del país de origen.

Si se permite que los datos fluyan libremente alrededor del mundo y los trabajadores no tienen asegurados sus derechos sobre protección de datos en la ley nacional o en acuerdos colectivos, el acceso y el control sobre los datos será todavía menor.

Ejemplo:

Los Teamsters en California habían negociado que los datos de localización de los conductores recolectados para garantizar su seguridad no pueden ser usados en evaluaciones de desempeño para estos trabajadores.

Descarga de datos

La última fase – la descarga de datos – esta conectada a la fase de almacenamiento, pero también se relaciona a la posible venta de datos/conjuntos de datos que incluyan datos de trabajadores. Los sindicatos deben mantenerse vigilantes. Se refiere a la posibilidad de borrar de datos, pero también a la venta y transferencia de conjuntos de datos, con inferencias y perfiles asociados, a terceros. Los sindicatos deberían ser incluidos en las negociaciones, con mucho mejores derechos para saber lo que está siendo descargado y para quién, con capacidad de objeción y bloqueo del proceso – esto es sumamente importante teniendo en vista las antes mencionadas negociaciones de comercio electrónico. Igualmente, los sindicatos deberían, como mínimo, tener el derecho de solicitar que los conjuntos de datos e inferencias sobre los trabajadores sean borrados cuando su propósito original fue alcanzado, de acuerdo con el principio de minimización de datos reconocido en el GDPR (artículo 5.1.c)[14].

13 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829
14 https://gdpr-info.eu/art-5-gdpr/
11 https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_112624.pdf
12 Article 35 du RGPD et Avis 2/2107 sur le traitement des données sur le lieu de travail du Groupe de travail «Article 29» sur la protection des données.
13 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829
14 https://gdpr-info.eu/art-5-gdpr/

Ejemplo:

El sindicato del sector financiero en Irlanda negoció dos artículos clave sobre políticas de personal en el banco – RBS:

1. Cláusula Anti-Mercantilización (Anti-Commodification Clause)
El banco se compromete a no transformar datos de trabajadores en productos para venta y comercialización.

2. Respeto a los Derechos Humanos
El banco se compromete a respetar la privacidad y los derechos humanos de los trabajadores como definidos en la ley, particularmente con consideración a la Declaración Universal de Derechos Humanos de la ONU y el Código de Prácticas para la Protección de Datos de Trabajadores de ILO en 1997.

Vea las publicaciones aquí.

Recomendaciones

Para proteger los derechos de los trabajadores en espacios de trabajo digitalizados y prevenir que muchas veces inferencias y perfiles de datos obscuros den forma a las oportunidades laborales de los trabajadores, los sindicatos deberían empezar a demandar y negociar muchos más y mejores derechos.

Para hacerlo, los sindicatos podrían:

1. Capacitar a los miembros y representantes sobre el papel de los datos en los espacios de trabajo digitalizados y en la sociedad como un todo. Esto incluye buenos consejos sobre el uso de aparatos provistos por los empleadores y buenas practicas sobre protección del derecho a privacidad afuera del horario laboral.
2. Considerar el establecimiento de un grupo de representantes especializados en la organización de datos del trabajo y de los trabajadores. Vea el Informe 2.
3. Tener recursos sindicales (expertos legales, unidades negociadoras y organizadores) que puedan apoyar las negociaciones mencionadas.
4. Negociar el ciclo de vida de los datos en el trabajo con una perspectiva basada en los derechos humanos y del trabajador.
5. Crear un cuadro de políticas de derechos sobre datos a nivel sindical que pueda informar representantes (digitales) en sus negociaciones. De acuerdo con los derechos humanos y con el ciclo de vida en el trabajo, podría contener artículos sobre:

   a. Principio general: Dignidad y bienestar durante el uso de tecnologías basadas en datos en el espacio de trabajo deberían ser aseguradas. Artículos y estándares que den a los trabajadores agencia sobre las nuevas tecnologías, y que promuevan salud y seguridad, protejan el derecho a la organización, guarden contra la discriminación o otros impactos negativos sobre los trabajadores deben ser establecidos.

   b. Trabajadores y/o sus representantes deberían estar involucrados en todas las evaluaciones de impacto y sus revisiones periódicas.

   c. Empleadores deberían notificar a los trabajadores de manera clara y accesible sobre todas las tecnologías de datos usadas en el espacio de trabajo. Las notificaciones deberían incluir una descripción entendible de la tecnología, los tipos de datos siendo colectados, los propósitos para el uso de los sistemas y los derechos y protecciones disponibles a los trabajadores.

d. Minimización de Datos: Empleadores deberían solamente colectar datos de los trabajadores cuando necesario y esencial para que hagan sus trabajos. Vea la definición en GDPR https://gdpr-info.eu/art-5-gdpr/

e. Trabajadores deberían tener el derecho al acceso, corrección y descarga de sus datos. Deberían recibir toda la información relevante con respecto a datos, incluyendo como y por que fue colectada, si hubo inferencias sobre los datos, y si sí cuales, si los datos fueron usados para decisiones relacionadas a empleo, incluyendo decisiones de contratos. Los empleadores deberían ser responsables por la corrección de datos equivocados.

f. Los datos de los trabajadores deberían estar seguramente guardados y protegidos del uso indebido. Particularmente, empleadores no deberían poder vender o licenciar/donar o dar acceso de alguna manera a los datos a terceros a los datos de los trabajadores; de lo contrario, el incentivo a la violación de la privacidad de los trabajadores vendiendo sus datos para obtener lucros monetarios es demasiado grande.

g. Las impresiones digitales y otros datos de salud no deberían nunca ser compartidos con terceros, solo si requerido por ley.

h. Empleadores deberían usar solamente sistemas de vigilancia con propósitos específicos que no dañen a los trabajadores (directa o indirectamente).

i. Cambios a los sistemas de vigilancia debido a cambios tecnológicos en el espacio de trabajo deberían ser sujetos a negociación colectiva.

j. Tecnologías de datos no deberían discriminar a los trabajadores con base en características protegidas como género, sexo, edad, discapacidad, matrimonio y estatus de unión civil, embarazo y maternidad, raza y creencia religiosa.

k. Eliminar características protegidas de las tecnologías de datos no debería automáticamente dar al empleador la capacidad de ignorar otros requerimientos en este cuadro de políticas. Por ejemplo, muchos empleadores justifican la venta o transferencia de conjuntos de datos que incluyen datos personales de trabajadores afirmando que los conjuntos de datos son anónimos y por eso no pueden ser conectados a los trabajadores individualmente. Sin embargo, muchos estudios muestran lo relativamente fácil que es de hacer visible la parte anónima de los conjuntos de datos[15] poniendo a la identidad y privacidad de los trabajadores en riesgo.

6. Ser cuidadoso y crítico con intentos de definir datos como productos/activos. Esto incluye sugestiones para diseños de sistemas de redistribución del valor adicional de los datos de vuelta a los trabajadores como medios de producción. Derechos no deberían ser intercambiados por dinero.

7. Considerar maneras responsables de colectar datos para contraprobar las análisis de la dirección (vea informe 3), y así rompiendo el monopolio de la "verdad" controlado por los empleadores.

15 https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAImZ_o2Up5jda586F7I4qomlzWnAvy7a3pbaQ4D8vXb7WB3oxaA-ZMJHNpXWZM9W0uCR8aCSvyqd-ZGaCWrugvxJ_y7GYlwTuv5Cysn4MvhjGmLmVg4uLwMjspp5cT1epXQCMYLMgIpNIzUzEW_MIBPjNEQWiUrQ7tBOTr8VIFXU