GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

17/ES

WP 249

Dictamen 2/2017 sobre el tratamiento de datos en el trabajo

Adoptado el 8 de junio de 2017

El Grupo de Trabajo se creó de conformidad con el artículo 29 de la Directiva 95/46/CE. Se trata de un órgano consultivo independiente de la UE en materia de protección de datos y privacidad. Sus funciones se describen en el artículo 30 de dicha Directiva y en el artículo 15 de la Directiva 2002/58/CE.

De su secretaría se ocupa la Dirección C (Derechos Fundamentales y Estado de Derecho) de la Dirección General de Justicia y Consumidores de la Comisión Europea, B-1049 Bruselas, Bélgica, Despacho MO59 05/35.

Sitio web: http://ec.europa.eu/justice/data-protection/index_en.htm

Índice

1 Resumen

El presente dictamen complementa las publicaciones anteriores del Grupo de Trabajo del Artículo 29 (GT29), el *Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral* (WP48)[1] y el *Documento de trabajo relativo a las comunicaciones electrónicas en el lugar de trabajo* (WP55) de 2002[2]. Desde la publicación de estos documentos, se han adoptado una serie de nuevas tecnologías que permiten un tratamiento más sistemático de los datos personales de los trabajadores en el trabajo, creando retos importantes para la intimidad y la protección de datos.

El presente dictamen reevalúa el equilibrio entre los intereses legítimos de los empresarios y las expectativas razonables de privacidad de los trabajadores, describiendo los riesgos que plantean las nuevas tecnologías y evaluando la proporcionalidad de una serie de escenarios en los que podrían aplicarse.

Aunque su objeto primordial es la Directiva sobre protección de datos, el dictamen se centra en las obligaciones adicionales que el Reglamento general de protección de datos impone a los empresarios. Asimismo, reitera la posición y las conclusiones del dictamen 8/2001 y del documento de trabajo WP55, a saber, que cuando se tratan datos personales de los trabajadores:

- los empresarios deben tener siempre presentes los principios fundamentales de protección de datos, independientemente de la tecnología utilizada;
- el contenido de las comunicaciones electrónicas realizadas desde establecimientos comerciales goza de la misma protección de los derechos fundamentales que las comunicaciones analógicas;
- es muy poco probable que el consentimiento constituya una base jurídica para el tratamiento de datos en el trabajo, a no ser que los trabajadores puedan negarse sin consecuencias adversas;
- en ocasiones, la ejecución de un contrato y los intereses legítimos pueden invocarse, siempre que el tratamiento sea estrictamente necesario para un fin legítimo y respete los principios de proporcionalidad y subsidiariedad;
- los trabajadores deben recibir información efectiva sobre el control que se lleva a cabo; y
- cualquier transferencia internacional de datos de los trabajadores únicamente debe efectuarse cuando esté garantizado un nivel adecuado de protección.

2. Introducción

La rápida adopción de las nuevas tecnologías de la información en el lugar de trabajo, en términos de infraestructura, aplicaciones y dispositivos inteligentes, permite nuevos tipos de tratamiento de datos sistemáticos y potencialmente invasivos. Por ejemplo:

---

[1] GT29, *Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral*, WP48, 13 de septiembre de 2001, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

[2] GT29, *Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo*, WP55, 29 de mayo de 2002, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_es.pdf

- en la actualidad, pueden aplicarse tecnologías que permiten el tratamiento de datos en el trabajo con un coste muy inferior al de hace varios años, mientras que la capacidad de tratamiento de datos personales de estas tecnologías ha aumentado exponencialmente;
- las nuevas formas de tratamiento, como las relativas a los datos personales sobre el uso de servicios en línea y/o los datos de localización de un dispositivo inteligente, son mucho menos visibles para los trabajadores que otros tipos más tradicionales, como las evidentes cámaras de televisión de circuito cerrado. Esto plantea interrogantes sobre hasta qué punto los trabajadores son conscientes de estas tecnologías, ya que los empresarios podrían llevar a cabo ilegalmente este tratamiento sin informarles previamente; y
- los límites entre el hogar y el lugar de trabajo se han ido difuminando cada vez más. Por ejemplo, cuando los trabajadores trabajan a distancia (desde su domicilio) o mientras viajan por motivos profesionales, puede llevarse a cabo un seguimiento de las actividades realizadas fuera del entorno físico de trabajo, que puede incluir el control del individuo en un contexto privado.

Por tanto, aunque el uso de estas tecnologías puede ser útil para detectar o prevenir la pérdida de propiedad intelectual y material de la empresa, mejorando la productividad de los trabajadores y protegiendo los datos personales de los que se encarga el responsable del tratamiento, también plantea importantes retos en materia de privacidad y protección de datos. Por consiguiente, se requiere una nueva evaluación del equilibrio entre el interés legítimo del empresario de proteger su empresa y la expectativa razonable de privacidad de los interesados: los trabajadores.

Aunque el presente dictamen se centra en las nuevas tecnologías de la información mediante la evaluación de nueve escenarios diferentes en los que pueden presentarse, también reflexiona brevemente sobre los métodos más tradicionales de tratamiento de datos en el trabajo, en los que los riesgos se agravan como consecuencia del cambio tecnológico.

Cuando en el presente dictamen se utiliza la palabra «trabajador», el GT29 no pretende limitar el ámbito de aplicación de este término únicamente a las personas con un contrato de trabajo reconocido como tal en la legislación laboral aplicable. En los últimos decenios, los nuevos modelos empresariales amparados por diferentes tipos de relaciones laborales y, en particular el trabajo por cuenta propia, se han hecho más habituales. El presente dictamen tiene por objeto cubrir todas las situaciones en las que existe una relación laboral, independientemente de si se basa o no en un contrato de trabajo.

Es importante señalar que, habida cuenta de la dependencia que resulta de la relación empresario/trabajador, este último rara vez está en condiciones de dar, denegar o revocar el consentimiento libremente. Salvo en situaciones excepcionales, los empresarios tendrán que basarse en otro fundamento jurídico distinto del consentimiento, como la necesidad de tratar los datos para su interés legítimo. Sin embargo, un interés legítimo en sí mismo no es suficiente para primar sobre los derechos y libertades de los trabajadores.

Independientemente de la base jurídica de dicho tratamiento, antes de su inicio se debe realizar una prueba de proporcionalidad con el fin de determinar si el tratamiento es necesario para lograr un fin legítimo, así como las medidas que deben adoptarse para garantizar que las violaciones de los derechos a la vida privada y al secreto de las comunicaciones se limiten al mínimo. Esto puede formar parte de una evaluación de impacto relativa a la protección de datos (EIPD).

3. Marco jurídico

Si bien el análisis que sigue a continuación se realiza principalmente en relación con el marco jurídico vigente en virtud de la Directiva 95/46/CE (Directiva sobre protección de datos o «DPD»)[3], el presente dictamen también tendrá en cuenta las obligaciones con arreglo al Reglamento 2016/679 (Reglamento general sobre protección de datos o «RGPD»)[4], que ya ha entrado en vigor y será aplicable a partir del 25 de mayo de 2018.

Respecto de la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas[5], el Grupo de Trabajo pide a los legisladores europeos que establezcan una excepción específica para la interferencia con los dispositivos que se entregan a los trabajadores[6]. La propuesta de Reglamento no incluye una excepción adecuada a la prohibición general de interferencia y, normalmente, los empresarios no pueden otorgar un consentimiento válido para el tratamiento de los datos personales de sus trabajadores.

3.1 Directiva 95/46/CE: Directiva sobre protección de datos («DPD»)

Con anterioridad, el GT29 indicó en el dictamen 8/2001, que los empresarios deben tener en cuenta los principios fundamentales relativos a la protección de datos de la DPD a la hora de tratar los datos personales en el contexto laboral. El desarrollo de nuevas tecnologías y métodos de tratamiento no han modificado esta situación; de hecho, puede decirse que estos avances hacen que sea *más* importante que los empresarios respeten dichos principios. En este contexto, los empresarios deben:

- garantizar que los datos se tratan con fines específicos y legítimos que sean proporcionados y necesarios;
- tener en cuenta el principio de limitación de la finalidad y al mismo tiempo asegurarse de que los datos sean adecuados, pertinentes y no excesivos para la finalidad legítima;
- aplicar los principios de proporcionalidad y subsidiariedad, independientemente del fundamento jurídico aplicable;
- ser transparentes con los trabajadores sobre el uso y la finalidad de las tecnologías de control;
- permitir el ejercicio de los derechos del interesado, incluidos el derecho de acceso y, en su caso, la rectificación, supresión o bloqueo de datos personales;
- mantener la exactitud de los datos y no conservarlos más tiempo del necesario; y

[3] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (*DO L 281 de 23.11.1995, p. 31*), http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:31995L0046.

[4] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (*DO L 119 de 4.5.2016, p. 1*), http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679.

[5] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE, 2017/0003/ (COD), http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017PC0010&from=ES

[6] Véase GT29, *Dictamen 01/2017 sobre la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas* (en inglés), WP 247 de 4 de abril de 2017, p. 29, http://ec.europa.eu/newsroom/document.cfm?doc_id=44103

- adoptar todas las medidas necesarias para proteger los datos contra el acceso no autorizado, así como garantizar que el personal conozca suficientemente las obligaciones en materia de protección de datos.

Sin repetir recomendaciones anteriores, el GT29 desea destacar tres principios, a saber: fundamentos jurídicos, transparencia y decisiones automatizadas.

3.1.1 *FUNDAMENTOS JURÍDICOS (ARTÍCULO 7)*

Cuando se tratan datos personales en el contexto laboral, debe cumplirse al menos uno de los criterios establecidos en el artículo 7. Si los tipos de datos personales tratados se refieren a las categorías especiales (según lo establecido en el artículo 8), el tratamiento está prohibido a menos que sea aplicable una excepción[7,8]. Incluso si el empresario puede invocar una de dichas excepciones, para que el tratamiento de datos sea legítimo, sigue siendo necesario uno de los fundamentos jurídicos establecidos en el artículo 7.

En resumen, los empresarios deben, por tanto, tomar nota de lo siguiente:

- para la mayoría de estos tratamientos de datos en el trabajo**, la base jurídica no puede y no debe ser el consentimiento de los trabajadores** [artículo 7, letra a)] debido a la naturaleza de la relación entre empresario y trabajador;
- el tratamiento puede ser necesario para **la ejecución de un contrato** [artículo 7, letra b)] en los casos en que el empresario deba tratar datos personales del trabajador para cumplir tales obligaciones;
- es bastante común que **el Derecho laboral pueda imponer obligaciones jurídicas** [artículo 7, letra c)] **que requieran el tratamiento de datos personales**; en tales casos, el trabajador debe estar clara y plenamente informado de dicho tratamiento (a menos que sea de aplicación una excepción);
- en caso de que un empresario pretenda invocar un **interés legítimo** [artículo 7, letra f)], la finalidad del tratamiento debe ser legítima; el método elegido o la tecnología específica deben ser necesarios, proporcionados y aplicados de la manera menos intrusiva posible, y el empresario deberá poder demostrar que **se han adoptado las medidas adecuadas** para garantizar un equilibrio con los derechos y libertades fundamentales de los trabajadores[9];
- las operaciones de tratamiento deben cumplir también los **requisitos de transparencia** (artículos 10 y 11), y los trabajadores deben estar clara y plenamente

[7] Como se establece en la parte 8 del dictamen 8/2001; por ejemplo, el artículo 8, apartado 2, letra b), establece una excepción al respeto de las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral, en la medida en que lo autorice una legislación nacional que prevea garantías adecuadas.

[8] Cabe señalar que en algunos países existen medidas especiales que los empresarios deben cumplir para proteger la vida privada de los trabajadores. Portugal es un ejemplo de país en el que existen estas medidas especiales y medidas similares podrían aplicarse también en otros Estados miembros. Por tanto, las conclusiones de la sección 5.6, así como los ejemplos presentados en las secciones 5.1 y 5.7.1 del presente dictamen no son válidas en Portugal por estas razones.

[9] GT29, *Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE*, WP 217, adoptado el 9 de abril de 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_es.pdf

informados del tratamiento de sus datos personales[10], incluida la existencia de cualquier control; y

- deben adoptarse **medidas técnicas y de organización adecuadas** con el fin de garantizar la seguridad del tratamiento (artículo 17).

Se detallan a continuación los criterios más pertinentes con arreglo al artículo 7.

- **Consentimiento [artículo 7, letra a)]**

El consentimiento, según la DPD, se define como toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan. Para que el consentimiento sea válido, también debe ser revocable.

El GT29 ha señalado anteriormente en el dictamen 8/2001 que cuando un empresario tiene que tratar datos personales de sus trabajadores, es engañoso partir del supuesto de que el tratamiento puede legitimarse a través del consentimiento de estos. En los casos que un empresario dice que requieren consentimiento y existe un perjuicio real o potencial relevante derivado del hecho de que el trabajador no consienta (lo cual puede ser muy probable en el contexto laboral, especialmente cuando el empresario hace un seguimiento del comportamiento del trabajador a lo largo del tiempo), entonces el consentimiento no es válido, ya que no es y no puede ser dado libremente. Por tanto, en la mayoría de los casos de tratamiento de datos de los trabajadores, la base jurídica de dicho tratamiento no puede y no debe ser el consentimiento de los trabajadores, por lo que se requiere una base jurídica diferente.

Además, incluso en los casos en que el consentimiento pueda considerarse una base jurídica válida de dicho tratamiento (es decir, si se puede concluir sin ninguna duda que el consentimiento se da libremente), este debe ser una manifestación específica e informada de la voluntad del trabajador. La configuración por defecto de los dispositivos y/o la instalación de programas informáticos que facilitan el tratamiento electrónico de datos personales no puede calificarse como consentimiento dado por los trabajadores, ya que el consentimiento requiere una manifestación activa de voluntad. La ausencia de acción (es decir, no cambiar la configuración por defecto) no se puede considerar, en general, como un consentimiento específico para permitir dicho tratamiento[11].

- **Ejecución de un contrato [artículo 7, letra b)]**

Las relaciones laborales se suelen basar en un contrato de trabajo entre el empresario y el trabajador. Para cumplir las obligaciones derivadas de este contrato, como pagar al trabajador, el empresario está obligado a tratar determinados datos personales.

- **Obligaciones jurídicas [artículo 7, letra c)]**

[10] De conformidad con el artículo 11, apartado 2, de la DPD, el responsable del tratamiento está exento de la obligación de comunicar información al interesado en los casos en los que el registro o la recopilación de datos estén expresamente prescritos por ley.

[11] Véase también GT29, *Dictamen 15/2011 sobre la definición del consentimiento,* WP187, 13 de julio de 2011, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_es.pdf, p. 24.

Es muy común que el Derecho laboral imponga obligaciones legales al empresario que requieren el tratamiento de datos personales (por ejemplo, para el cálculo de impuestos y la gestión de los salarios). Evidentemente, en tales casos, dicha ley constituye la base jurídica para el tratamiento de datos.

- **Interés legítimo [artículo 7, letra f)]**

Si un empresario desea invocar el fundamento jurídico del artículo 7, letra f), de la DPD, la finalidad del tratamiento debe ser legítima y el método elegido o la tecnología específica para llevar a cabo el tratamiento deben ser necesarios para el interés legítimo del empresario. El tratamiento también debe ser proporcional a las necesidades de la empresa, es decir, a la finalidad que pretende abordar. El tratamiento de datos en el lugar de trabajo debe llevarse a cabo de la manera menos intrusiva posible y estar dirigido al ámbito de riesgo específico. Además, conforme al artículo 7, letra f), el trabajador conserva el derecho a oponerse al tratamiento por razones legítimas convincentes con arreglo al artículo 14.

Para invocar el artículo 7, letra f), como fundamento jurídico para el tratamiento es esencial que existan medidas específicas de mitigación con el fin de garantizar un equilibrio adecuado entre el legítimo interés del empresario y los derechos y libertades fundamentales de los trabajadores[12]. Tales medidas, dependiendo de la forma de control, deberían incluir limitaciones con el fin de garantizar que no se viole la privacidad del trabajador. Estas limitaciones podrían:

- ser geográficas (por ejemplo, control únicamente en lugares específicos; debe prohibirse el control en zonas sensibles como lugares religiosos y, por ejemplo, zonas de aseos y salas de descanso),
- estar orientadas a datos (por ejemplo, los archivos electrónicos personales y las comunicaciones no deben ser controlados), y
- ser temporales (por ejemplo, muestreo en lugar de control continuo).

3.1.2 *TRANSPARENCIA (ARTÍCULOS 10 Y 11)*

Los requisitos de transparencia de los artículos 10 y 11 se aplican al tratamiento de datos en el trabajo; se debe informar a los trabajadores de la existencia de cualquier control y de los fines para los cuales se tratarán los datos personales, y debe aportarse cualquier otra información necesaria para garantizar un tratamiento leal.

Con las nuevas tecnologías, la necesidad de transparencia se hace más evidente, ya que permiten la recogida y el tratamiento posterior de posiblemente grandes cantidades de datos personales de forma encubierta.

3.1.3 *DECISIONES AUTOMATIZADAS (ARTÍCULO 15)*

[12] Como ejemplo del equilibrio que debe lograrse, véase el asunto de Köpke/Alemania, [2010] ECHR 1725, (http://www.bailii.org/eu/cases/ECHR/2010/1725.html), en el que un trabajador fue despedido como resultado de una operación de videovigilancia discreta llevada a cabo por el empresario y una agencia de detectives privados. Aunque en este caso el Tribunal concluyó que las autoridades nacionales habían logrado un equilibrio justo entre los intereses legítimos del empresario (protección de sus derechos de propiedad), el derecho del trabajador al respeto de la vida privada y el interés público en la administración de justicia, también observó que los distintos intereses afectados podrían valorarse de manera diferente en el futuro como resultado del desarrollo tecnológico.

El artículo 15 de la DPD también reconoce el derecho de los interesados a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, a menos que la decisión sea necesaria para la celebración o ejecución de un contrato, esté amparada por el Derecho de la Unión o de un Estado miembro o se base en el consentimiento explícito del interesado.

3.2 Reglamento 2016/679: Reglamento general de protección de datos («RGPD»)

El RGPD incluye y refuerza los requisitos de la DPD. Además, introduce nuevas obligaciones para todos los responsables del tratamiento de datos, incluidos los empresarios.

3.2.1 *PROTECCIÓN DE DATOS DESDE EL DISEÑO*

El artículo 25 del RGDP establece que los responsables del tratamiento deberán aplicar la protección de datos desde el diseño y por defecto. Por ejemplo: si un empresario entrega dispositivos a los trabajadores, si se trata de tecnologías de seguimiento, deben seleccionarse las soluciones más respetuosas con la privacidad. Asimismo, debe tenerse en cuenta la minimización de datos.

3.2.2 *EVALUACIONES DE IMPACTO RELATIVAS A LA PROTECCIÓN DE DATOS*

El artículo 35 del RGPD señala los requisitos para que un responsable del tratamiento realice una evaluación de impacto relativa a la protección de datos (EIPD) cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas. Un ejemplo es el caso de la evaluación sistemática y exhaustiva de aspectos personales relacionados con las personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las persona físicas o que les afecten significativamente de modo similar.

Si la EIPD indica que el responsable del tratamiento no puede abordar debidamente los riesgos identificados, es decir, que los riesgos residuales siguen siendo elevados, entonces dicho responsable debe consultar a la autoridad de control antes de proceder al tratamiento (artículo 36, apartado 1), tal como se aclara en las directrices del GT29 sobre las EIPD[13].

3.2.2 *TRATAMIENTO EN EL ÁMBITO LABORAL*

El artículo 88 del RGPD dispone que los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de:

- contratación;
- ejecución del contrato laboral (incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo);

[13] GT29, *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679* (en inglés), WP 248, 4 de abril de 2017, http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, p. 18.

- gestión, planificación y organización del trabajo;
- igualdad y diversidad en el lugar de trabajo;
- salud y seguridad en el trabajo,
- protección de los bienes de empresarios o clientes;
- ejercicio y disfrute (individual) de los derechos y prestaciones relacionados con el empleo; y
- extinción de la relación laboral.

De conformidad con el artículo 88, apartado 2, dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a:

- la transparencia del tratamiento;
- la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta; y
- los sistemas de supervisión en el lugar de trabajo.

En el presente dictamen, el Grupo de Trabajo orienta sobre la utilización legítima de las nuevas tecnologías en una serie de situaciones concretas, detallando medidas adecuadas y específicas para salvaguardar la dignidad humana, los intereses legítimos y los derechos fundamentales de los trabajadores.

4. Riesgos

Las tecnologías modernas permiten que los trabajadores puedan ser objeto de seguimiento a lo largo del tiempo, en los lugares de trabajo y en sus hogares, a través de muchos dispositivos diferentes, como teléfonos inteligentes, ordenadores de mesa, tabletas, vehículos y tecnología ponible. Si el tratamiento no tiene límites y no es transparente, existe un alto riesgo de que el interés legítimo de los empresarios en la mejora de la eficiencia y protección de los activos de la empresa se convierta en un control injustificado e intrusivo.

Las tecnologías que controlan las comunicaciones también pueden tener un efecto desalentador sobre los derechos fundamentales de los trabajadores a organizarse, convocar reuniones de trabajadores y comunicarse de forma confidencial (incluido el derecho a buscar información). El control de las comunicaciones y del comportamiento ejercerá una presión coercitiva sobre los trabajadores para evitar la detección de lo que podría percibirse como anomalías, de manera comparable a la forma en que el uso intensivo de cámaras de televisión ha influido en el comportamiento de los ciudadanos en los espacios públicos. Además, debido a las capacidades de estas tecnologías, es posible que los trabajadores no sepan qué datos personales se están tratando y para qué fines, aunque también es posible que ni siquiera conozcan la existencia de la propia tecnología de control.

El control del uso de las tecnologías de la información también difiere de otras herramientas de observación y control más visibles, como las cámaras de televisión, ya que puede tener lugar de forma encubierta. A falta de una política de control fácilmente comprensible y de fácil acceso en el lugar de trabajo, los trabajadores pueden no ser conscientes de la existencia y las consecuencias del control que se está llevando a cabo y, por tanto, podrían no ejercer sus derechos. Otro riesgo se deriva de la excesiva recogida de datos en dichos sistemas, por ejemplo, aquellos que recogen datos de localización WiFi.

El aumento de la cantidad de datos generados en el entorno del lugar de trabajo, en combinación con las nuevas técnicas de análisis de datos y la comparación cruzada, también puede crear el riesgo de un tratamiento posterior incompatible. Ejemplos de tratamiento posterior ilegítimo incluyen el uso de sistemas instalados legítimamente para proteger las propiedades para controlar después la disponibilidad, el desempeño y el trato de los trabajadores con los clientes. Otros incluyen el uso de los datos recopilados a través de un sistema de circuito cerrado de televisión para controlar regularmente el comportamiento y el rendimiento de los trabajadores, o el uso de datos de un sistema de geolocalización (por ejemplo, seguimiento mediante WiFi o Bluetooth) para comprobar constantemente los movimientos y el comportamiento de un trabajador.

Como resultado, este seguimiento puede infringir los derechos de privacidad de los trabajadores, independientemente de que el control se lleve a cabo de forma sistemática u ocasional. El riesgo no se limita al análisis del contenido de las comunicaciones. Por tanto, el análisis de metadatos sobre una persona podría permitir un control igualmente invasivo y detallado de su vida y pautas de comportamiento.

El uso amplio de tecnologías de control también puede limitar la disposición de los trabajadores a informar a los empresarios (y los canales por los cuales podrían hacerlo) sobre irregularidades o acciones ilegales de superiores y otros trabajadores que puedan suponer un daño para la empresa (especialmente los datos de los clientes) o el lugar de trabajo. El anonimato suele ser necesario para que un trabajador actúe y denuncie tales situaciones. El control que infringe el derecho a la privacidad de los trabajadores puede obstaculizar las comunicaciones necesarias con los responsables apropiados. En ese caso, los medios establecidos para los denunciantes internos pueden resultar ineficaces[14].

5. Escenarios

Esta sección aborda una serie de escenarios de tratamiento de datos en el trabajo en los que nuevas tecnologías o mejoras de las tecnologías existentes tienen, o pueden tener, el potencial de derivar en riesgos elevados para la privacidad de los trabajadores. En todos estos casos, los empresarios deberían considerar si:

- la actividad de tratamiento es necesaria y, en caso afirmativo, los fundamentos jurídicos aplicables;
- el tratamiento de propuesto de los datos personales es leal para los trabajadores;
- la actividad de tratamiento es proporcional a las inquietudes planteadas; y
- la actividad de tratamiento es transparente.

5.1 Operaciones de tratamiento durante el proceso de selección

El uso de redes sociales por parte de los individuos está muy extendido y es relativamente común que los perfiles de usuario sean visibles públicamente, dependiendo de la configuración elegida por el titular de la cuenta. En consecuencia, los empresarios podrían

[14] Véase, por ejemplo, GT29, *Dictamen 1/2006 relativo a la aplicación de las normas sobre protección de datos de la UE a los sistemas internos de denuncia de irregularidades en los ámbitos de la contabilidad, controles de auditoría internos, cuestiones de auditoría, lucha contra la corrupción y delitos financieros y bancarios*, WP 117, 1 de febrero de 2006, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_es.pdf.

creer que la inspección de los perfiles sociales de los posibles candidatos durante el proceso de selección puede estar justificada. Este puede ser también el caso de otra información de acceso público relativa al trabajador potencial.

Sin embargo, los empresarios no deben asumir que simplemente porque el perfil de una persona en las redes sociales es de acceso público, está permitido que traten esos datos para sus propios fines. Para este tratamiento se requiere un fundamento jurídico, como el interés legítimo. En este contexto, el empresario debe, antes de inspeccionar un perfil de redes sociales, tener en cuenta si el perfil del solicitante está relacionado con fines profesionales o privados, ya que esto podría ser un indicio importante sobre la admisibilidad jurídica de la inspección de los datos. Además, los empresarios solo podrán recoger y tratar datos personales relativos a los solicitantes de empleo en la medida en que la recopilación de estos datos sea necesaria y pertinente para el desempeño del trabajo solicitado.

Los datos recopilados durante el proceso de selección deberían, en general, suprimirse tan pronto como quede claro que no se hará una oferta de empleo a la persona en cuestión o que esta la rechazará[15]. Asimismo, la persona debe ser correctamente informada sobre cualquier tratamiento antes de iniciar el proceso de selección.

No existe ningún fundamento jurídico para que un empresario solicite «amistad» a trabajadores potenciales o para que estos, por otros medios, proporcionen acceso a los contenidos de sus perfiles.

Ejemplo

Durante la selección de nuevo personal, un empresario comprueba los perfiles de los candidatos en varias redes sociales e incluye información de estas redes (y cualquier otra información disponible en Internet) en el proceso de selección.

Solo si para el puesto de trabajo es necesario revisar la información sobre un candidato en las redes sociales, por ejemplo, para poder evaluar los riesgos específicos de los candidatos respecto de una función específica y los candidatos están correctamente informados (por ejemplo, en el texto del anuncio de trabajo), el empresario puede tener una base jurídica en virtud del artículo 7, letra f), para revisar la información de acceso público relativa a los candidatos.

5.2 Operaciones de tratamiento derivadas del examen en el empleo

A través de la existencia de perfiles en las redes sociales y del desarrollo de nuevas tecnologías analíticas, los empresarios tienen (o pueden obtener) la capacidad técnica para examinar de forma permanente a los trabajadores mediante la recopilación de información sobre sus amigos, opiniones, creencias, intereses, hábitos, paraderos, actitudes y comportamientos, captando así datos, incluidos datos sensibles, relacionados con la vida privada y familiar del trabajador.

[15] Véase también, *Recommendation CM/Rec(2015)5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment* del Consejo de Europa, párrafo 13.2, 1 de abril de 2015, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a). En los casos en los que el empresario desee guardar los datos con vistas a otras ofertas de trabajo, se debe informar en consecuencia al interesado y ofrecerle la oportunidad de oponerse a dicho tratamiento posterior, en cuyo caso la información debe suprimirse.

El examen por las empresas de los perfiles en las redes sociales de sus trabajadores no debe realizarse de forma generalizada.

Además, los empresarios deben abstenerse de solicitar a un trabajador o a un solicitante de empleo acceso a información que este comparta con otras personas a través de las redes sociales.

Ejemplo

Un empresario sigue los perfiles de LinkedIn de sus extrabajadores con cláusulas de no competencia durante el período de vigencia de estas con el fin de controlar el cumplimiento de dichas cláusulas. El control se limita a estos extrabajadores.

Siempre que el empresario pueda demostrar que dicho control es necesario para proteger sus intereses legítimos, que no existen otros medios menos invasivos y que los extrabajadores han sido adecuadamente informados del alcance del control periódico de sus comunicaciones públicas, podrá acogerse a la base jurídica del artículo 7, letra f), de la DPD.

Asimismo, no se deberá exigir a los trabajadores que utilicen un perfil de redes sociales facilitado por su empresario. Incluso cuando ello esté previsto de forma específica debido a sus tareas (por ejemplo, portavoz de una organización), los trabajadores deben conservar la opción de un perfil «no profesional» y no público que puedan utilizar en lugar del perfil «oficial» relacionado con el empresario, y esto debería especificarse en el contrato de trabajo.

5.3 Operaciones de tratamiento derivadas de la vigilancia del uso de las TIC en el lugar de trabajo

Tradicionalmente, se consideraba que el control de las comunicaciones electrónicas en el lugar de trabajo (teléfono, navegación por Internet, correo electrónico, mensajería instantánea, VoIP, etc.) era la principal amenaza para la privacidad de los trabajadores. En su *Documento de trabajo relativo a las comunicaciones electrónicas en el lugar de trabajo* de 2001, el GT29 formuló una serie de conclusiones en relación con el control del correo electrónico y la utilización de Internet. Si bien esas conclusiones siguen siendo válidas, es necesario tener en cuenta los avances tecnológicos que han permitido formas de control más nuevas, potencialmente más intrusivas y generalizadas. Estos avances incluyen, entre otros:

- herramientas de prevención de pérdida de datos (DLP), que controlan las comunicaciones salientes con el fin de detectar posibles violaciones de la seguridad de los datos;
- cortafuegos de próxima generación (NGFW) y sistemas de gestión unificada de amenazas (UTM), que pueden proporcionar una variedad de tecnologías de control, entre ellas la inspección profunda de paquetes, interceptación TLS, filtrado de sitios web, filtrado de contenido, informes sobre dispositivos, información de identidad de usuario y (como se describió anteriormente) prevención de pérdida de datos. Estas tecnologías también pueden utilizarse individualmente, dependiendo del empresario;
- aplicaciones y medidas de seguridad que impliquen registrar el acceso de los trabajadores a los sistemas del empresario;
- tecnología de detección electrónica (eDiscovery), es decir, cualquier proceso de búsqueda de datos electrónicos con el fin de utilizarlos como prueba;

- seguimiento del uso de la aplicación y el dispositivo a través de programas informáticos ocultos, ya sea en el ordenador o en la nube;
- uso en el lugar de trabajo de aplicaciones de oficina proporcionadas como servicio en la nube que, en teoría, permiten un registro muy detallado de las actividades de los trabajadores;
- control de los dispositivos personales (por ejemplo, ordenadores personales, teléfonos móviles, tabletas), que los trabajadores aportan para su trabajo, de acuerdo con una política de uso específico, como la de que el trabajador utilice su propio dispositivo, y tecnología de gestión de sistemas móviles, que permite la distribución de aplicaciones, datos y ajustes de configuración y parches para dispositivos móviles; y
- uso de dispositivos ponibles (por ejemplo, dispositivos de salud y estado físico).

Es posible que un empresario pueda aplicar una solución de control única, tal como un conjunto de paquetes de seguridad que le permita controlar todo el uso de las TIC en el lugar de trabajo, en vez de controlar solo el correo electrónico y/o el sitio web, como sucedía antes. Las conclusiones adoptadas en el WP55 se aplicarían a cualquier sistema que permita este control[16].

Ejemplo

Un empresario tiene la intención de utilizar un dispositivo de inspección TLS para descifrar e inspeccionar el tráfico seguro, con el fin de detectar cualquier elemento malicioso. El dispositivo también es capaz de registrar y analizar toda la actividad en línea de un trabajador en la red de la organización.

Con el fin proteger los flujos de datos en línea relacionados con datos personales contra la interceptación, el uso de comunicaciones cifradas es cada vez más frecuente. Sin embargo, esto también puede presentar problemas, ya que el cifrado imposibilita controlar los datos entrantes y salientes. El equipo de inspección TLS descifra el flujo de datos, analiza el contenido con fines de seguridad y, a continuación, lo vuelve a cifrar.

En este ejemplo, el empresario invoca intereses legítimos: la necesidad de proteger la red y los datos personales de los trabajadores y clientes que allí se guardan contra el acceso no autorizado o la fuga de datos. Sin embargo, el control de todas las actividades en línea de los trabajadores es una respuesta desproporcionada y una injerencia en el derecho al secreto de las comunicaciones. El empresario debe explorar, en primer lugar, otros medios menos invasivos para proteger la confidencialidad de los datos del cliente y la seguridad de la red.

En la medida en que alguna interceptación del tráfico TLS pueda calificarse como estrictamente necesaria, el dispositivo debe configurarse de forma que se evite el registro permanente de la actividad del trabajador, por ejemplo, bloqueando el tráfico entrante o saliente sospechoso y redireccionando al usuario a un portal de información en el que pueda solicitar la revisión de dicha decisión automatizada. No obstante, si se considerara estrictamente necesario realizar algún registro general, el dispositivo también puede

[16] Véase también Copland/ Reino Unido, (2007) 45 EHRR 37, 25 BHRC 216, 2 ALR Int'l 785, [2007] ECHR 253 (http://www.bailii.org/eu/cases/ECHR/2007/253.html), en la que el Tribunal afirmó que los correos electrónicos enviados desde establecimientos comerciales y la información derivada del control del uso de Internet podían formar parte de la vida privada y la correspondencia de un trabajador, y que la recogida y el almacenamiento de esa información sin su conocimiento constituiría una injerencia en sus derechos, aunque el Tribunal no dictaminó que esta vigilancia no sería nunca necesaria en una sociedad democrática.

configurarse para no almacenar datos de registro a menos que el dispositivo señale la ocurrencia de un incidente, con una reducción al mínimo de la información recopilada.

Como buena práctica, el empresario podría ofrecer a los trabajadores un acceso alternativo no controlado. Esto podría hacerse ofreciendo WiFi gratis, o dispositivos o terminales independientes (con las debidas salvaguardias para garantizar la confidencialidad de las comunicaciones) con los que los trabajadores puedan ejercer su derecho legítimo a utilizar las instalaciones de trabajo para algún uso privado[17]. Además, los empresarios deberían considerar ciertos tipos de tráfico cuya interceptación ponga en peligro el equilibrio adecuado entre sus intereses legítimos y la privacidad del trabajador –como el uso del correo electrónico privado, la banca en línea y los sitios web de salud– con el objetivo de configurar adecuadamente el dispositivo, de modo que no se proceda a la interceptación de comunicaciones en circunstancias que no cumplan la proporcionalidad. La información sobre el tipo de comunicaciones que el aparato controla debe especificarse a los trabajadores.

Debería elaborarse una política sobre los fines respecto de cuándo y quién puede acceder a datos de registro sospechosos, que sea de acceso fácil y permanente para todos los trabajadores, a fin de orientarlos también sobre el uso aceptable e inaceptable de la red y las instalaciones. Esto permite que los trabajadores adapten su comportamiento para evitar que se les controle cuando utilizan legítimamente los servicios de tecnologías de la información del trabajo para uso privado. Como buena práctica, dicha política debería evaluarse, al menos anualmente, con el fin de valorar si la solución de control elegida ofrece los resultados previstos y si existen otros instrumentos o medios menos invasivos para lograr los mismos fines.

Independientemente de la tecnología o de las capacidades que posea, la base jurídica del artículo 7, letra f), solo está disponible si el tratamiento cumple determinadas condiciones. En primer lugar, los empresarios que utilicen estos productos y aplicaciones deben tener en cuenta la proporcionalidad de las medidas que apliquen y, si es posible, adoptar medidas adicionales para mitigar o reducir la escala y el impacto del tratamiento de los datos. Como ejemplo de buena práctica, esta consideración podría llevarse a cabo a través de una EIPD antes de la introducción de cualquier tecnología de control. En segundo lugar, los empresarios deben aplicar y comunicar políticas de uso aceptables, junto con políticas de privacidad, que indiquen el uso permisible de la red y los equipos de la organización, y que detallen de manera rigurosa el tratamiento que se está llevando a cabo.

En algunos países, la formulación de una política de este tipo requeriría legalmente la aprobación de un comité de empresa o una representación similar de los trabajadores. En la práctica, el personal de mantenimiento informático suele elaborar estas políticas. Dado que su principal interés será sobre todo la seguridad y no la expectativa legítima de privacidad de los trabajadores, el GP29 recomienda que, en todos los casos, una muestra representativa de trabajadores participe en la evaluación de la necesidad del control, así como en la lógica y accesibilidad de la política.

[17] Véase Halford/ Reino Unido, [1997] ECHR 32, (http://www.bailii.org/eu/cases/ECHR/1997/32.html), en la que se afirma que «las llamadas telefónicas realizadas desde establecimientos comerciales, así como desde el hogar pueden estar contempladas en los conceptos de "vida privada" y "correspondencia" en el sentido del artículo 8, apartado 1 [del Convenio]»; y Barbulescu/Rumanía, [2016] ECHR 61, (http://www.bailii.org/eu/cases/ECHR/2016/61.html), en relación con el uso de una cuenta de mensajería instantánea profesional para la correspondencia personal, en la que el Tribunal afirmó que el control de la cuenta por parte del empresario era limitada y proporcional, aunque con el voto particular del juez Pinto de Alberquerque, que abogaba por un equilibrio prudente.

Ejemplo

Un empresario utiliza una herramienta de prevención de pérdida de datos para controlar automáticamente los correos electrónicos salientes, con el fin de prevenir la transmisión no autorizada de datos protegidos (por ejemplo, datos personales del cliente), independientemente de si dicha acción es involuntaria o no. Cuando se considera que un correo electrónico es fuente potencial de una violación de la confidencialidad de los datos, se realiza una investigación adicional.

Una vez más, el empresario se basa en la necesidad para su interés legítimo de proteger los datos personales de los clientes, así como sus activos contra el acceso no autorizado o la fuga de datos. Sin embargo, dicha herramienta DLP puede implicar un tratamiento de datos personales innecesario, por ejemplo, una alerta de «falso positivo» puede dar lugar a un acceso no autorizado a correos electrónicos legítimos enviados por los trabajadores (que pueden ser, por ejemplo, correos electrónicos personales).

Por tanto, la necesidad de la herramienta DLP y su utilización deben estar plenamente justificadas para lograr el equilibrio adecuado entre sus intereses legítimos y el derecho fundamental a la protección de los datos personales de los trabajadores. Para que se puedan invocar los intereses legítimos del empresario, deben adoptarse determinadas medidas para mitigar los riesgos. Por ejemplo, las reglas que el sistema sigue para definir un correo electrónico como posible violación de la confidencialidad de los datos deben ser completamente transparentes para los usuarios y, en el caso de que la herramienta reconozca un correo electrónico que se va a enviar como posible violación de datos, un mensaje de advertencia debe informar al remitente del correo electrónico antes de su transmisión, a fin de ofrecerle la opción de cancelar dicha transmisión.

En algunos casos, el control de los trabajadores es posible no tanto por el despliegue de tecnologías específicas, sino simplemente porque se espera que utilicen aplicaciones en línea puestas a disposición por el empresario que tratan datos personales. El uso de aplicaciones de oficina basadas en la nube (por ejemplo, editores de documentos, calendarios, redes sociales) es un ejemplo de ello. Debe garantizarse que los trabajadores puedan designar determinados espacios privados a los que el empresario no pueda tener acceso salvo en circunstancias excepcionales. Esto, por ejemplo, es pertinente para los calendarios, que también se suelen utilizar para citas privadas. Si el trabajador programa una cita como «privada» o lo anota como tal, los empresarios (y otros trabajadores) no deberían estar autorizados para ver el contenido de la cita.

El requisito de subsidiariedad en este contexto significa, en ocasiones, que no puede tener lugar ningún tipo de control. Por ejemplo, este es el caso cuando se puede prevenir el uso prohibido de servicios de comunicación mediante el bloqueo de ciertos sitios web. Si es posible bloquear los sitios web, en lugar de controlar todas las comunicaciones de forma continuada, para cumplir este requisito de subsidiariedad se debe elegir el bloqueo.

De manera más general, la prevención debería tener mucho más peso que la detección: prevenir el uso indebido de Internet mediante medios técnicos resulta más beneficioso para los intereses del empresario que invertir recursos en detectarlo.

5.4 Operaciones de tratamiento derivadas de la observación del uso de las TIC fuera del lugar de trabajo

El uso de las TIC fuera del lugar de trabajo se ha vuelto más común con el crecimiento de las políticas de trabajo a domicilio, trabajo a distancia y de utilización por el trabajador de su propio dispositivo. Las capacidades de estas tecnologías pueden suponer un riesgo para la vida privada de los trabajadores, ya que, en muchos casos, los sistemas de control existentes en el lugar de trabajo se extienden de manera efectiva a la esfera doméstica de los trabajadores cuando utilizan estos equipos.

5.4.1 *OBSERVACIÓN DEL TRABAJO A DOMICILIO Y REMOTO*

Cada vez es más común que los empresarios ofrezcan a los trabajadores la opción de trabajar a distancia, por ejemplo, desde casa y/o durante el traslado. De hecho, esto es un factor central que explica la poca diferenciación entre lugar de trabajo y hogar. En general, se trata de que el empresario entregue equipos o programas informáticos a los trabajadores que, una vez instalados en su hogar o en sus propios dispositivos, les permitan tener el mismo nivel de acceso a la red, los sistemas y los recursos que tendrían si estuvieran en el lugar de trabajo, en función de la aplicación.

Aunque el trabajo a distancia puede ser una evolución positiva, también presenta un tipo de riesgo adicional para el empresario. Por ejemplo, los trabajadores que tienen acceso remoto a la infraestructura del empresario no están sujetos a las medidas de seguridad física que existen en las instalaciones del empresario. Dicho claramente: sin la aplicación de las medidas técnicas adecuadas, el riesgo de acceso no autorizado aumenta y puede dar lugar a la pérdida o destrucción de información, incluidos los datos personales de trabajadores o clientes de los que pueda disponer el empresario.

Con el fin de mitigar este tipo de riesgo, los empresarios pueden pensar que existe una justificación para utilizar paquetes de programas informáticos (ya sea en las instalaciones o en la nube) que tengan la capacidad de, por ejemplo, registrar pulsaciones en el teclado y movimientos del ratón, capturas de pantalla (ya sea al azar o a intervalos determinados), registrar las aplicaciones utilizadas (y durante cuánto tiempo se utilizaron) y, en dispositivos compatibles, habilitar las cámaras web y recopilar secuencias de las mismas. Estas tecnologías están ampliamente disponibles, incluso por parte de terceros, como los proveedores de servicios en la nube.

Sin embargo, el tratamiento que implican estas tecnologías es desproporcionado y es muy poco probable que el empresario tenga un fundamento jurídico en virtud del interés legítimo, por ejemplo, para registrar las pulsaciones en el teclado y los movimientos del ratón de un trabajador.

La clave está en abordar el riesgo que supone el trabajo a domicilio y a distancia de forma proporcionada y no excesiva, sea cual fuere la opción que se ofrezca y la tecnología que se proponga, en particular si los límites entre el uso profesional y privado son fluidos.

5.4.2 *UTILIZACIÓN DEL PROPIO DISPOSITIVO DEL TRABAJADOR* BRING YOUR OWN DEVICE (BYOD)

Debido al aumento de la popularidad, las funcionalidades y la capacidad de los dispositivos electrónicos de consumo, los empresarios pueden enfrentarse a peticiones de los trabajadores de utilizar sus propios dispositivos en el lugar de trabajo para llevar a cabo sus tareas.

Aplicar esta posibilidad de manera eficaz puede dar lugar a una serie de beneficios para los trabajadores, como la mejora de la satisfacción en el trabajo, el aumento de la moral en

general, el aumento de la eficiencia en el trabajo y una mayor flexibilidad. Sin embargo, el uso del dispositivo de un trabajador será personal por naturaleza, y esto es más probable que ocurra en ciertos momentos del día (por ejemplo, por la noche y los fines de semana). Por tanto, es posible que el uso de sus propios dispositivos por parte de los trabajadores conduzca a que los empresarios traten información extraempresarial sobre ellos y, posiblemente, sobre cualquier miembro de la familia que también utilice los dispositivos.

En el contexto laboral, los riesgos de privacidad de la utilización del propio dispositivo del trabajador se asocian comúnmente a tecnologías de control que recogen identificadores como direcciones MAC, o en casos en los que un empresario accede al dispositivo de un trabajador con la justificación de realizar un análisis de seguridad, es decir, para detectar programas informáticos malintencionados. Respecto de esto último, existen varias soluciones comerciales que permiten el escaneo de dispositivos privados, aunque su uso podría permitir el acceso a todos los datos de ese dispositivo y, por tanto, deben gestionarse cuidadosamente. Por ejemplo, en principio, no se puede acceder a las secciones de un dispositivo que se supone que solo se utilizan con fines privados (por ejemplo, la carpeta que almacena las fotos tomadas con el dispositivo).

Se puede considerar que el control de la localización y el tráfico de dichos dispositivos sirve al interés legítimo de proteger los datos personales de los que el empresario está a cargo como responsable del tratamiento; sin embargo, esto puede ser ilegal en lo que respecta al dispositivo personal de un trabajador, si dicho control también captura datos relativos a su vida privada y familiar. Con el fin de evitar la observación de información privada, deben adoptarse medidas adecuadas para distinguir entre el uso privado y profesional del dispositivo.

Los empresarios también deben poner en práctica métodos mediante los cuales sus propios datos del dispositivo se transfieran de forma segura entre ese dispositivo y su red. Puede darse el caso de que el dispositivo esté, por tanto, configurado para dirigir todo el tráfico a través de una red privada virtual (VPN) de vuelta hacia la red de la empresa, con el fin de ofrecer un cierto nivel de seguridad; sin embargo, si se utiliza esta medida, el empresario también debe tener en cuenta que el programa informático instalado con fines de control representa un riesgo para la privacidad durante los períodos de uso personal por parte del trabajador. Podrían utilizarse dispositivos que ofrezcan protecciones adicionales, como los datos en *sandboxing* (mantenimiento de los datos contenidos dentro de una aplicación específica).

Por el contrario, el empresario también debe tener en cuenta la prohibición del uso de dispositivos específicos del trabajo para uso privado si no hay manera de impedir la observación del uso privado, por ejemplo, si el dispositivo ofrece acceso remoto a datos personales de los que el empresario es el responsable del tratamiento.

5.4.3 *GESTIÓN DE DISPOSITIVOS MÓVILES (MDM)*

La gestión de dispositivos móviles permite a los empresarios localizar dispositivos de forma remota, utilizar configuraciones y/o aplicaciones específicas y borrar datos previa petición. Un empresario puede gestionar esta funcionalidad por sí mismo, o utilizar a un tercero para hacerlo. Los servicios de MDM también permiten que los empresarios registren o sigan el dispositivo instantáneamente, incluso si no se ha denunciado su robo.

Debe realizarse una EIPD antes de utilizar cualquier tecnología de este tipo cuando para el responsable del tratamiento sea nueva o desconocida. Si el resultado de la EIPD es que la tecnología MDM es necesaria en circunstancias específicas, aún debe evaluarse si el tratamiento de datos resultante cumple los principios de proporcionalidad y subsidiariedad. Los empresarios deben asegurarse de que los datos recogidos como parte de esta capacidad de localización remota se traten con un fin específico y no formen parte de un programa más amplio que permita la observación continua de los trabajadores. Incluso para los fines especificados, las funciones de seguimiento deben mitigarse. Los sistemas de seguimiento se pueden diseñar para registrar los datos de localización sin presentarlos al empresario. En tales circunstancias, los datos de localización deben estar disponibles únicamente cuando el dispositivo sea objeto de denuncia o se pierda.

Los trabajadores cuyos dispositivos estén inscritos en los servicios de MDM también deben ser plenamente informados sobre el seguimiento llevado a cabo y las consecuencias que esto tiene para ellos.

5.4.4 *DISPOSITIVOS PONIBLES*

Los empresarios están cada vez más tentados de dotar a sus trabajadores con dispositivos que se pueden llevar puestos para tener un control de su salud y actividad dentro y, a veces, incluso fuera del lugar de trabajo. Sin embargo, esto implica el tratamiento de datos de salud, por lo que está prohibido con arreglo al artículo 8 de la DPD.

Dada la relación desigual entre empresarios y trabajadores (pues el trabajador tiene una dependencia financiera del empresario) y la naturaleza sensible de los datos de salud, es muy improbable que se pueda dar un consentimiento legal explícito para el seguimiento u observación de estos datos, ya que, en primer lugar, los trabajadores no son esencialmente «libres» para dar dicho consentimiento. Incluso si el empresario utiliza a un tercero para recopilar los datos de salud, que solo proporcionarían al empresario información agregada sobre la evolución general en este ámbito, el tratamiento seguiría siendo ilegal.

Asimismo, como se señala en el *Dictamen 5/2014 sobre técnicas de anonimización*[18], es técnicamente muy difícil garantizar la anonimización completa de los datos. Incluso en un entorno con más de mil empleados, habida cuenta de la disponibilidad de otros datos sobre los trabajadores, el empresario aún podría distinguir a los trabajadores individuales con indicadores de salud particulares, como hipertensión u obesidad.

Ejemplo:

Una organización ofrece a sus trabajadores dispositivos de seguimiento del estado físico como regalo. Los dispositivos cuentan el número de pasos que los trabajadores dan y registra sus latidos y patrones de sueño a lo largo del tiempo.

Los datos de salud resultantes solo deberían ser accesibles para el trabajador y no para el empresario. Cualquier dato transferido entre el trabajador (como interesado) y el proveedor del dispositivo/servicio (como responsable del tratamiento) es una cuestión que compete a ambas partes.

[18] GT29, *Dictamen 5/2014 sobre técnicas de anonimización*, WP 216, 10 de abril de 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf

Habida cuenta de que los datos de salud también podrían ser objeto de tratamiento por la parte comercial que haya fabricado los dispositivos u ofrezca un servicio a los empresarios, el empresario, a la hora de elegir el dispositivo o servicio, debe evaluar la política de privacidad del fabricante y/o proveedor de servicios, con el fin de asegurarse de que no se produzca un tratamiento ilícito de los datos de salud de los trabajadores.

5.5 Operaciones de tratamiento relacionadas con el empleo del tiempo y la presencia

Los sistemas que permiten a los empresarios controlar quién puede entrar en sus instalaciones, y/o en ciertas zonas de sus instalaciones, también pueden permitir el seguimiento de las actividades de los trabajadores. Aunque estos sistemas existen desde hace años, las nuevas tecnologías destinadas a hacer un seguimiento del empleo del tiempo y la presencia de los trabajadores se están generalizando, incluidas las que tratan datos biométricos y otras como el seguimiento de dispositivos móviles.

Aunque estos sistemas pueden constituir un componente importante del seguimiento efectuado por el empresario, también plantean el riesgo de proporcionar un nivel invasivo de conocimientos y control sobre las actividades del trabajador en el lugar de trabajo.

Ejemplo:

Un empresario dispone de una sala de servidores en la que se almacenan en formato digital datos sensibles de la empresa, datos personales de los trabajadores y datos personales de los clientes. Para cumplir las obligaciones legales de proteger los datos contra el acceso no autorizado, el empresario ha instalado un sistema de control de acceso que registra la entrada y salida de los trabajadores que tienen permiso para entrar en la sala. Si desaparecen elementos del equipo o algún dato es objeto de acceso no autorizado, pérdida o robo, los registros guardados por el empresario le permiten determinar quién tuvo acceso a la sala en ese momento.

Habida cuenta de que el tratamiento es necesario y no prima sobre el derecho a la vida privada de los trabajadores, este puede ser en el interés legítimo con arreglo al artículo 7, letra f), si los trabajadores han sido informados adecuadamente sobre la operación de tratamiento. Sin embargo, la observación continua de la frecuencia y los tiempos exactos de entrada y salida de los trabajadores no puede justificarse si estos datos se utilizan también para otros fines, como la evaluación del desempeño.

5.6 Operaciones de tratamiento con sistemas de videovigilancia

La videovigilancia sigue presentando los mismos problemas para la privacidad de los trabajadores que antes: la capacidad de grabar de forma continuada el comportamiento del trabajador[19]. Los cambios más relevantes relacionados con la aplicación de esta tecnología en el contexto del empleo son la capacidad de acceder fácilmente a los datos recogidos a distancia (por ejemplo, a través de un teléfono inteligente), la reducción de los tamaños de las cámaras (junto con un aumento de sus capacidades, por ejemplo, de alta definición) y el tratamiento que pueden realizar los nuevos análisis de vídeo.

[19] Véase el asunto mencionado Köpke/Alemania; además, cabe señalar también que en algunas jurisdicciones, la instalación de sistemas como los circuitos cerrados de cámaras de televisión con el fin de probar una conducta ilícita ha sido declarada admisible; véase el asunto Bershka en el Tribunal Constitucional de España.

Con las capacidades que ofrecen los análisis de vídeo, es posible que un empresario observe las expresiones faciales del trabajador por medios automatizados, identifique desviaciones con respecto a los patrones de movimiento predefinidos (por ejemplo, una fábrica), etc. Esto sería desproporcionado a efectos de los derechos y libertades de los trabajadores y, por tanto, ilegal en general. El tratamiento también puede implicar la elaboración de perfiles y, posiblemente, la toma de decisiones automatizada. Por tanto, los empresarios deben abstenerse de utilizar tecnologías de reconocimiento facial. Puede haber algunas excepciones marginales a esta regla, pero tales escenarios no pueden utilizarse para invocar una legitimación general del uso de esta tecnología[20].

5.7 Operaciones de tratamiento que implican vehículos utilizados por los trabajadores

Las tecnologías que permiten a los empresarios controlar sus vehículos se han generalizado, en particular entre las organizaciones cuyas actividades implican el transporte o que tienen grandes flotas de vehículos.

Cualquier empresario que utilice la telemática de vehículos recopilará datos sobre el vehículo y el trabajador que lo utiliza. Estos datos pueden incluir no solo la localización del vehículo (y, por tanto, del trabajador) recogida por los sistemas de seguimiento por GPS básicos, sino también, dependiendo de la tecnología, una gran cantidad de otra información, incluyendo el comportamiento al volante. Ciertas tecnologías también pueden permitir la observación continua tanto del vehículo como del conductor (por ejemplo, los registradores de datos de incidencias).

Un empresario puede estar obligado a instalar una tecnología de seguimiento en los vehículos para demostrar el cumplimiento de otras obligaciones legales, por ejemplo garantizar la seguridad de los trabajadores que los conducen. También puede tener un interés legítimo en poder localizar los vehículos en cualquier momento. Incluso si los empresarios tuvieran un interés legítimo para lograr estos fines, en primer lugar se debería evaluar si el tratamiento es necesario para dichos fines y si la aplicación efectiva cumple los principios de proporcionalidad y subsidiariedad. Cuando se permite el uso privado de un vehículo profesional, la medida más importante que puede tomar un empresario para garantizar el cumplimiento de estos principios es ofrecer una exclusión voluntaria: en principio, el trabajador debe tener la posibilidad de desactivar temporalmente el seguimiento de la localización cuando lo justifiquen circunstancias especiales, como la visita a un médico. De esta manera, el trabajador puede proteger por iniciativa propia determinados datos de la localización como privados. El empresario debe asegurarse de que los datos recopilados no se utilicen para un tratamiento posterior ilegítimo, como el seguimiento y la evaluación de los trabajadores.

El empresario también debe informar claramente a los trabajadores de que se ha instalado un dispositivo de seguimiento en el vehículo de la empresa que conducen, y que sus movimientos están siendo registrados mientras lo utilizan (y que, en función de la tecnología utilizada, también puede registrarse su comportamiento al volante). Preferiblemente, esta información debería aparecer en un lugar destacado de cada vehículo, a la vista del conductor.

[20] Además, con arreglo al RGPD, el tratamiento de datos biométricos con fines de identificación debe basarse en una de las excepciones previstas en el artículo 9, apartado 2.

Es posible que los trabajadores puedan utilizar los vehículos de la empresa fuera del horario de trabajo, por ejemplo, para uso personal, dependiendo de las políticas específicas que rijan el uso de dichos vehículos. Dada la sensibilidad de los datos de localización, es poco probable que exista una base jurídica para controlar la ubicación de los vehículos de los trabajadores fuera de las horas de trabajo acordadas. Sin embargo, si esta necesidad existiera, debe considerarse una utilización que sea proporcional al riesgo. Por ejemplo, esto podría significar que, para prevenir el robo de automóviles, la localización del automóvil no se registre fuera de las horas de trabajo, a menos que el vehículo salga de una zona ampliamente definida (región o incluso país). Además, la localización únicamente se mostraría como último recurso: el empresario solo podría activar la «visibilidad» de la localización, accediendo a los datos ya almacenados por el sistema cuando el vehículo salga de una región predefinida.

Como se afirmó en el *Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes*[21] del GT29:

> «Los dispositivos de seguimiento de vehículos no son dispositivos para la localización de trabajadores, ya que su función es hacer un seguimiento o vigilar la ubicación de los vehículos en que estén instalados. Los empresarios no deben considerarlos como dispositivos para seguir o el comportamiento o el paradero de los conductores o de otro tipo de personal, por ejemplo, mediante el envío de alertas relacionadas con la velocidad del vehículo».

Asimismo, como se indica en el *Dictamen 5/2005 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido*[22] del GT29:

> «El tratamiento de los datos de localización puede estar justificado si se lleva a cabo formando parte del control del transporte de personas o bienes o de la mejora de la distribución de los recursos para servicios en puntos remotos (por ejemplo, la planificación de operaciones en tiempo real) o cuando se trate de lograr un objetivo de seguridad en relación con el propio empleado o con los bienes o vehículos a su cargo. Por el contrario, el Grupo considera que el tratamiento de datos es excesivo en el caso de que los empleados puedan organizar libremente sus planes de viaje o cuando se lleve a cabo con el único fin de controlar el trabajo de un empleado, siempre que pueda hacerse por otros medios».

5.7.1 REGISTRADOR DE DATOS DE INCIDENCIAS

Los registradores de datos de incidencias ofrecen a un empresario la capacidad técnica de procesar una cantidad significativa de datos personales sobre los trabajadores que conducen vehículos de la empresa. Estos dispositivos se colocan cada vez más en los vehículos con el objeto de grabar vídeos, e incluso sonido, en caso de accidente. Estos sistemas son capaces de grabar en determinados momentos, por ejemplo en respuesta a frenadas repentinas, cambios bruscos de dirección o accidentes, en los que se almacenan los momentos inmediatamente anteriores al incidente, pero también se pueden configurar para controlar de forma continua. Esta información puede utilizarse posteriormente para observar y revisar el comportamiento

[21] GT29, *Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes,* WP 185, 16 de mayo de 2011, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_es.pd

[22] GT29, *Dictamen 5/2005 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido*, WP 115, 25 de noviembre de 2005, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_es.pdf

al volante de una persona con el fin de mejorarlo. Además, muchos de estos sistemas incluyen GPS para hacer un seguimiento de la ubicación instantánea del vehículo y también se pueden almacenar otros detalles correspondientes a la conducción (como la velocidad) para su posterior tratamiento.

Estos dispositivos se han generalizado particularmente en las organizaciones cuyas actividades implican el transporte o tienen flotas importantes de vehículos. Sin embargo, la utilización de registradores de datos de incidencias únicamente puede ser lícita si existe la necesidad de tratar los datos personales del trabajador para un fin legítimo y si el tratamiento cumple los principios de proporcionalidad y subsidiariedad.

Ejemplo

Una empresa de transporte equipa todos sus vehículos con una cámara de vídeo dentro de la cabina que graba sonido y vídeo. El objetivo del tratamiento de estos datos es mejorar las habilidades de conducción de los trabajadores. Las cámaras están configuradas para conservar grabaciones de los momentos en que se producen incidentes como frenazos repentinos o cambios bruscos de dirección. La empresa asume que tiene un fundamento jurídico para el tratamiento en su interés legítimo con arreglo al artículo 7, letra f), de la Directiva, con el fin de proteger la seguridad de sus trabajadores y la de los demás conductores.

Sin embargo, el interés legítimo de la empresa de controlar a los conductores no prevalece sobre los derechos de estos últimos a la protección de sus datos personales. El control continuo de los trabajadores con estas cámaras constituye una grave injerencia en su derecho a la privacidad. Existen otros métodos (por ejemplo, la instalación de equipos que impiden el uso de teléfonos móviles) y sistemas de seguridad, como un sistema avanzado de frenado de emergencia o un sistema de advertencia de abandono del carril, que pueden utilizarse para la prevención de accidentes de vehículos, y que pueden ser más adecuados. Además, un vídeo de este tipo tiene una alta probabilidad de dar lugar al tratamiento de datos personales de terceros (como los peatones) y, para tal tratamiento, el interés legítimo de la empresa no es suficiente justificación.

5.8 Operaciones de tratamiento que implican la comunicación de datos de los trabajadores a terceros

Resulta cada vez más habitual que las empresas transmitan los datos de sus trabajadores a sus clientes con el fin de garantizar una prestación de servicios fiable. Estos datos pueden ser excesivos dependiendo del alcance de los servicios prestados (por ejemplo, se puede incluir la foto de un empleado). Sin embargo, los trabajadores no están en condiciones, habida cuenta del desequilibrio de poder, de dar su libre consentimiento al tratamiento de sus datos personales por parte de su empresario, y si el tratamiento de los datos no es proporcional, el empresario no tiene un fundamento jurídico.

Ejemplo:

Una empresa de mensajería envía a sus clientes un correo electrónico con un enlace al nombre y la ubicación del repartidor (empleado). La empresa también pretendía adjuntar una foto de pasaporte del repartidor. La empresa suponía que tenía un fundamento jurídico para el tratamiento en su interés legítimo [artículo 7, letra f), de la Directiva], que permitiría al cliente comprobar si el repartidor es efectivamente la persona correcta.

Sin embargo, no es necesario facilitar el nombre y la foto del repartidor a los clientes. Dado que no existe ningún otro motivo legítimo para este tratamiento, la empresa de mensajería no está autorizada a facilitar estos datos personales a los clientes.

5.9 Operaciones de tratamiento que implican transferencias internacionales de datos de recursos humanos y otros datos de trabajadores

Los empresarios recurren cada vez más a aplicaciones y servicios basados en la nube, como los diseñados para la gestión de datos de recursos humanos y las aplicaciones de oficina en línea. El uso de la mayoría de estas aplicaciones dará lugar a la transferencia internacional de datos relativos a los trabajadores. Como ya se señaló en el Dictamen 8/2001, el artículo 25 de la Directiva establece que las transferencias de datos personales a un tercer país fuera de la UE únicamente pueden efectuarse cuando dicho país garantice un nivel de protección adecuado. Cualquiera que sea la base, la transferencia debe cumplir las disposiciones de la Directiva.

Por tanto, debe garantizarse el cumplimiento de estas disposiciones relativas a la transferencia internacional de datos. El GT29 reafirma su posición anterior de que es preferible basarse en una protección adecuada en lugar de en las excepciones enumeradas en el artículo 26 de la DPD; cuando se recurra al consentimiento, este debe ser específico, inequívoco y libre. No obstante, también debe garantizarse que los datos compartidos fuera de la UE/EEE, y el consiguiente acceso por otras entidades del grupo, permanezcan limitados al mínimo necesario para los fines previstos.

6. Conclusiones y recomendaciones

6.1 Derechos fundamentales

Los contenidos de las comunicaciones mencionadas, así como los datos de tráfico relativos a dichas comunicaciones, gozan de la misma protección de los derechos fundamentales que las comunicaciones «analógicas».

Las comunicaciones electrónicas realizadas desde establecimientos comerciales pueden estar contempladas en los conceptos de «vida privada» y «correspondencia» en el sentido del artículo 8, apartado 1, del Convenio Europeo. Basándose en la actual Directiva sobre protección de datos, los empresarios solo podrán recoger datos para fines legítimos y el tratamiento se llevará a cabo en condiciones adecuadas (por ejemplo, proporcionadas y necesarias, para un interés real y presente, de forma lícita, articulada y transparente), con una base jurídica para el tratamiento de datos personales recogidos o generados a través de comunicaciones electrónicas.

El hecho de que un empresario sea propietario de los medios electrónicos no excluye el derecho de los trabajadores a mantener en secreto sus comunicaciones, los datos de localización relacionados y la correspondencia. El seguimiento de la localización de los trabajadores a través de sus propios dispositivos o de los dispositivos entregados por la empresa debe limitarse a lo estrictamente necesario para un fin legítimo. Ciertamente, en el caso de que el trabajador utilice su propio dispositivo es importante que tenga la oportunidad de proteger sus comunicaciones privadas de cualquier observación relacionada con el trabajo.

6.2 Consentimiento e interés legítimo

Los trabajadores casi nunca están en condiciones de dar, denegar o revocar el consentimiento libremente, habida cuenta de la dependencia que resulta de la relación empresario/trabajador. Dado el desequilibrio de poder, los trabajadores solo pueden dar su libre consentimiento en circunstancias excepcionales, cuando la aceptación o el rechazo de una oferta no tiene consecuencias.

El interés legítimo de los empresarios puede invocarse, en ocasiones, como fundamento jurídico, pero solo si el tratamiento es estrictamente necesario para un fin legítimo y cumple los principios de proporcionalidad y subsidiariedad. Debería realizarse una prueba de proporcionalidad antes de la utilización de cualquier herramienta de observación para determinar si todos los datos son necesarios, si este tratamiento prevalece sobre los derechos generales de privacidad que los trabajadores tienen también en el lugar de trabajo y qué medidas deben adoptarse para garantizar que las violaciones del derecho a la vida privada y el derecho al secreto de las comunicaciones se limiten al mínimo necesario.

6.3 Transparencia

Deberá comunicarse efectivamente a los trabajadores cualquier control que se lleve a cabo, sus fines y circunstancias, así como las posibilidades de que los trabajadores eviten que las tecnologías de control capturen sus datos. Las políticas y normas relativas al control legítimo deben ser claras y de fácil acceso. El Grupo de Trabajo recomienda que una muestra representativa de trabajadores participe en la elaboración y evaluación de dichas normas y políticas, ya que la mayoría de los controles pueden vulnerar la vida privada de estos.

6.4 Proporcionalidad y minimización de datos

El tratamiento de datos en el trabajo debe ser una respuesta proporcionada a los riesgos a los que se enfrenta un empresario. Por ejemplo, el uso indebido de Internet se puede detectar sin necesidad de analizar el contenido del sitio web. Si el uso indebido se puede prevenir (por ejemplo, mediante el uso de filtros web) el empresario no tiene ningún derecho general de control.

Además, una prohibición general de las comunicaciones por razones personales es poco práctica y su aplicación puede requerir un nivel de control desproporcionado. La prevención debería tener mucho más peso que la detección: prevenir el uso indebido de Internet mediante medios técnicos resulta más beneficioso para los intereses del empresario que invertir recursos en detectarlo.

La información registrada procedente del control, así como la información que se muestra al empresario, debe minimizarse en la medida de lo posible. Los trabajadores deben tener la posibilidad de interrumpir temporalmente el seguimiento de la localización, si las circunstancias lo justifican. Pueden diseñarse soluciones para que, por ejemplo, el seguimiento de vehículos registre los datos de posición sin presentarlos al empresario.

Los empresarios deben tener en cuenta el principio de minimización de los datos a la hora de decidir sobre la utilización de nuevas tecnologías. La información debe almacenarse durante el tiempo mínimo necesario, con un período de retención especificado. Cuando la información ya no sea necesaria debe ser eliminada.

6.5 Servicios en la nube, aplicaciones en línea y transferencias internacionales

Cuando se espere que los trabajadores utilicen aplicaciones en línea que traten datos personales (como las aplicaciones de oficina en línea), los empresarios deben considerar la posibilidad de permitir que los trabajadores designen ciertos espacios privados a los que el empresario no puede tener acceso bajo ninguna circunstancia, como un correo privado o una carpeta de documentos.

El uso de la mayoría de las aplicaciones en la nube dará lugar a la transferencia internacional de datos de los trabajadores. Debe garantizarse que las transferencias de datos personales a un tercer país fuera de la UE únicamente se efectúen cuando esté garantizado un nivel adecuado de protección y que los datos compartidos fuera de la UE/EEE y el consiguiente acceso por otras entidades del grupo se limite al mínimo necesario para los fines previstos.

* * *

Hecho en Bruselas, el 8 de junio de 2017

Por el Grupo de Trabajo
La presidenta
Isabelle FALQUE-PIERROTIN