Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en Protección de Datos

La privacidad del trabajador frente al control empresarial del correo electrónico corporativo

Trabajo fin de estudio presentado por:	Lucía Gil Vallilengua
Tipo de trabajo:	Trabajo Fin de Máster
Director/a:	Susana Duro Carrión
Fecha:	26/06/2024

Resumen

En los últimos años, la digitalización de los puestos de trabajo, por un lado, y el auge del teletrabajo, por otro, han ocasionado que buena parte de los trabajadores del mercado laboral desempeñen su actividad mediante una herramienta de trabajo principal y, en muchos casos, única: el ordenador.

En este escenario, las empresas han ido implementando nuevas formas de supervisión del cumplimiento de las obligaciones laborales centradas, fundamentalmente, en el control de los equipos informáticos puestos a disposición del empleado. No obstante, estas nuevas formas de control suscitan, a nivel jurídico, no pocos interrogantes.

En este trabajo, nos centraremos en el acceso por parte del empresario al correo electrónico y a los sistemas de mensajería corporativos, analizando el conflicto que esta medida puede plantear entre el derecho a la privacidad del empleado y la libertad de empresa de la organización. Determinaremos la legitimidad o no de este control a través de la jurisprudencia, la doctrina y la posición de la Agencia Española de Protección de Datos. Y, finalmente, analizaremos las implicaciones que puede tener su uso inapropiado, tanto en relación con la validez de la prueba en procedimientos judiciales como en relación con las responsabilidades generadas al empresario.

Palabras clave: control empresarial, relación laboral, privacidad del trabajador, protección de datos, intimidad, secreto de las comunicaciones, correo electrónico

Abstract

In recent years, the digitalization of jobs, on the one hand, and the rise of teleworking, on the other, have caused a large part of the workers in the labor market to carry out their activity through a main work tool and, in many cases, only: the computer.

In this scenario, companies have been implementing new forms of supervision of compliance with labor obligations focused, fundamentally, on the control of computer equipment made available to the employee. However, these new forms of control raise, at a legal level, many questions.

In this work, we will focus on the employer's access to email and corporate messaging systems, analyzing the conflict that this measure may pose between the employee's right to privacy and the organization's freedom of business. We will determine the legitimacy or otherwise of this control through jurisprudence, doctrine and the position of the Spanish Data Protection Agency. And, finally, we will analyze the implications that its inappropriate use may have, both in relation to the validity of the evidence in judicial procedures and in relation to the responsibilities generated by the employer.

Keywords: business control, employment relationship, worker privacy, data protection, privacy, secrecy of communications, email

Índice de contenidos

"*Calidad significa hacer lo correcto,*
cuando nadie está mirando"
Henry Ford, empresario

1. Introducción

Si hay algo que hace una persona a lo largo de su vida, es, muy probablemente, trabajar. El mundo laboral, ya sea desde la perspectiva del trabajador, ya desde la del empresario, es una realidad que afecta a prácticamente a la totalidad de la población. A su vez, una inmensa mayoría de los puestos trabajos utilizan herramientas informáticas que, hoy en día, se han consagrado como básicas para el desarrollo de las funciones laborales. Una de ellas es el correo electrónico. Éste es uno de los medios de comunicación interna y externa preferidos de las empresas en España y, precisamente por ello, constituye uno de los elementos principales de control del empresario para verificar el adecuado desempeño del trabajador.

No obstante, el correo electrónico, creado en 1971 (GARCÍA HERNANDEZ 2011) y con más de 50 años de historia, también está dejando paso a otras herramientas corporativas de comunicación como *Slack* o *Teams* que cada vez se encuentran más presentes en las empresas y que, por ello, también son objeto de supervisión por parte del empleador.

En todo caso, la misma evolución tecnológica que penetra en las organizaciones y facilita sus procesos, también ha traído consigo medidas de control tecnológicas más intrusivas en la intimidad del trabajador que requieren una sosegada revisión por parte de la comunidad doctrinal.

1.1. Justificación del tema elegido

Si bien en trabajos de investigación previos, ha llamado mi atención la intimidad personal y la protección de datos del individuo, en esta ocasión, siguiendo con esta línea pero concretando en una condición habitual de aquel, la de trabajador, he querido ahondar en cómo se modulan estos derechos fundamentales dentro de la particular relación empleado-empresario.

Dentro de todos los mecanismos de control que se pueden implementar en una organización, he seleccionado el correo electrónico y las herramientas de comunicación interna de la empresa por dos razones. Por un lado, por su constante y asentado uso en los puestos de trabajo. Y, por otro, por el debate jurídico existente tanto en el ámbito judicial como en la

doctrina ante las lagunas legales que, pese a los intentos normativos de los últimos años, sigue habiendo.

1.2. Problema y finalidad del trabajo

Con el presente trabajo, se tratará de exponer la compleja relación existente entre la privacidad del trabajador y la facultad de control del empresario. Una relación que no ha sido resuelta por la normativa vigente, por lo que ha quedado en manos de los tribunales la elaboración de una serie de criterios para ponderar los derechos en juego.

De esta forma, con la finalidad de abordar el estado de la cuestión y extraer conclusiones que permitan ofrecer una suerte de seguridad jurídica ante las carencias normativas concurrentes, repasaremos la posición de la doctrina y la jurisprudencia respecto al control del correo electrónico por parte del empleador. Igualmente, estudiaremos la supervisión empresarial sobre otros sistemas de comunicación empresarial y analizaremos cómo pueden tener encaje en el marco jurisprudencial creado, fundamentalmente, para el tradicional correo electrónico. En todo este camino, también hallaremos la importancia de un derecho tradicionalmente olvidado en este ámbito, el derecho a la autodeterminación informativa, y apuntaremos cómo este derecho resulta afectado en la implementación de mecanismos de control de las comunicaciones.

1.3. Objetivos

A continuación, se presentan los objetivos del presente trabajo:

1.3.1. Objetivo general

- Concluir en qué casos el control del correo electrónico corporativo u otras herramientas similares, por parte del empleador, es legal.

1.3.2. Objetivos específicos

- Revisar qué derechos fundamentales se encuentran afectados por el control en el correo electrónico

- Determinar en qué casos existe una "expectativa de privacidad" por parte del trabajador y si ésta puede ser completamente eliminada
- Recopilar los requisitos formales y materiales para que el control del correo electrónico esté amparado en Derecho
- Estudiar la legalidad de la vigilancia encubierta del correo electrónico
- Examinar las aplicaciones de mensajería instantánea más utilizadas y verificar su encaje en el marco normativo y jurisprudencial aplicable
- Revisar las algunas de las opciones de *software* para el control de empleados que ofrece el mercado y valorar si respetan la privacidad del trabajador
- Analizar las consecuencias en cuanto al valor probatorio de las evidencias obtenidas a través del control empresarial de las comunicaciones del empleado
- Revisar la responsabilidad que surge del uso inadecuado de los sistemas de control de comunicaciones internas de la empresa

2. Marco teórico y desarrollo

Para poder determinar si el control del correo electrónico por parte del empresario a sus trabajadores es lícito, se hace necesaria la revisión del marco jurídico y jurisprudencial aplicable. A estos efectos, y a salvo de evitar cualquier expectativa de sencillez en el asunto, se debe adelantar que control del correo electrónico de un trabajador – o de los sistemas de comunicación corporativa que cada empresa utilice - constituye una medida compleja desde el punto de vista jurídico, en primer término, por el número de derechos afectados. No sólo resulta involucrado el derecho a la intimidad del trabajador o a la protección de datos, sino también un tercer derecho fundamental: el secreto de las comunicaciones.

Además, comprobaremos que, lamentablemente, no existe una normativa específica que recoja esta problemática y un minucioso estudio de la jurisprudencia nos va a llevar a una fórmula que, aunque ayuda a ponderar los derechos enfrentados, dista mucho de solventar la conflictividad que cada día se presenta. Esta fórmula es el conocido test de proporcionalidad (que aúna los juicios de idoneidad, necesidad y el de proporcionalidad en sentido estricto). No obstante, la necesaria aplicación de este test en el caso concreto lleva a que sea sensiblemente

complejo extrapolar conclusiones a nuevos supuestos que, sin duda, presentarán notas diferenciadoras, sin poder, así, alcanzar conclusiones absolutas.

2.1. Potestad de control del empleador

El primer punto en el que debemos adentrarnos es la potestad de control del empleador y cómo está regulada en el marco normativo español. Enraizada en el artículo 38 de la Carta Magna y regulada en el art. 20.3 del Estatuto de los Trabajadores, esta potestad permite a todo empresario adoptar cuantas medidas de vigilancia y control considere precisas a fin de verificar el cumplimiento de las obligaciones laborales asumidas por el trabajador. Pensar que, entre esas medidas, puede encontrarse el control del correo electrónico, es algo lógico debido a la configuración digital de la mayor parte de los trabajos actuales.

Quizá, lo más relevante de cómo se ha recogido esta facultad empresarial, a la vista del presente trabajo, es que el citado precepto contiene una suerte de principio de "finalidad" que viene determinado por comprobar que la actividad laboral del trabajador es correcta, pero, y aquí aparece el primer límite de este derecho, respetando en todo caso la dignidad del trabajador, lo que también remite al respeto a la intimidad (Sentencia del Tribunal Superior de Justicia de Andalucía de 12 de julio de 2017).

Si nos fijamos, el artículo expresamente indica que estas medidas han de tener como finalidad la de comprobar que la actividad laboral se realiza adecuadamente por el trabajador. Este aspecto es notablemente significativo pues implica que otras finalidades no serían lícitas o no se encontrarían sujetas a las limitaciones del precepto por no estar incluidas en su ámbito objetivo. Este sería el caso, por ejemplo, de mantener la seguridad IT de la empresa. En este supuesto, para proteger la seguridad y los datos de la organización, las empresas pueden controlar el correo electrónico del trabajador a través de herramientas de prevención de pérdida de datos (DLP) que controlan las comunicaciones salientes para detectar incidencias de seguridad, cortafuegos (NGFW) y sistemas de gestión unificada de amenazas (UTM) que, para realizar sus funciones, también pueden acceder al correo electrónico. Otro supuesto que quedaría fuera del art. 20.3 ET, sería la adopción de medidas de control para el cumplimiento de una obligación legal, como pudiera ser para garantizar el derecho a la desconexión digital incluido en el art. 88 LOPDGDD.

Pero además del art. 20.3, gracias a la Disposición Final 13 de la Ley Orgánica 3/2018, de 5 de diciembre de Protección de los Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD), encontramos el art. 20 bis sobre los "Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión". En este precepto, se reconoce que los empleados tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición. No obstante, y aunque su inclusión puede considerarse beneficiosa por mencionar una problemática existente desde hace años en sede judicial, no deja de resultar vacía de contenido pues no especifica de modo alguno los límites que presenta ese espacio de intimidad del trabajador.

De esta forma, para poder dilucidar los contornos de la intimidad y la privacidad del trabajador en el uso del equipo que le ha sido facilitado, y concretamente respecto a los sistemas de comunicación empresariales, debemos salir del Estatuto de los Trabajadores y analizar el origen: cuáles son los derechos fundamentales afectados.

2.2. Derechos fundamentales afectados en el control del correo electrónico

Como se ha dicho, resulta obligatorio revisar los tres derechos fundamentales que quedan afectados ante la medida empresarial de control del correo del empleado.

Aunque hemos indicado que son tres, la jurisprudencia ha venido centrándose, casi exclusivamente, en uno de ellos, el derecho fundamental a la intimidad, dejando a los otros dos relegados, ya sea por la posterior atención y desarrollo legal que ha tenido uno de ellos (el derecho fundamental a la protección de datos), ya por la restrictiva aplicación que requiere el otro (secreto de las comunicaciones). No obstante, esa sesgada atención que tradicionalmente se ha prestado al conflicto no anula la existencia de estos derechos del lado del trabajador, ni la presencia de las obligaciones que suponen en el del empresario.

2.2.1. Secreto de las comunicaciones

De entre todos los elementos que el empleador puede controlar y que pueden afectar en mayor o menor medida a la intimidad y, en su caso, a la propia imagen, sólo el control del correo electrónico puede involucrar al secreto de las comunicaciones recogido en el art.18.3 CE. Esto es sumamente relevante porque la Constitución sólo levanta esta inviolabilidad cuando un juez así lo determina. Por ello, la doctrina ha apuntado a que la vigilancia empresarial del correo es una de las más polémicas (LUNA HUERTAS, MARTÍNEZ LÓPEZ, INFANTE MORO, 2003, p. 17).

Hoy en día, los tribunales reconocen que el trabajador, frente a la vigilancia de su correo, cuenta con una protección adicional que deriva de la garantía constitucional del secreto de las comunicaciones. Así lo han recogido, entre otras, la Sentencia del Tribunal Supremo de 26 de septiembre de 2007 o de 8 de marzo de 2011. No obstante, esto no siempre ha sido así.

Jurisprudencia no tan reciente, sin embargo, ha cuestionado que este derecho se estuviera conculcando toda vez que el uso del correo se realiza por cuenta del empresario. Ejemplo de ello es la Sentencia del Tribunal Superior de Justicia de Andalucía de 9 de mayo de 2003 que señalaba que, tratándose de sistemas de comunicación de la empresa, la comunicación a través de ellos no permitía considerar al empresario como ajeno, salvo que el empresario permitiese, de manera expresa, usar estos medios para fines distintos al trabajo. Ello, sobre la base de que esas comunicaciones se realizaban a través de un medio puesto a disposición por la empresa para desarrollar el objeto de trabajo y durante las horas de la jornada laboral.

En esta misma línea, algún autor ha considerado que el secreto de las comunicaciones, en el ámbito de las relaciones laborales, tiene una virtualidad cuanto menos discutible o circunstancial, lo que tiene una notable incidencia en el tema que estamos tratando, pues para realizar un control sobre el correo electrónico del trabajador, se dejaría de estar bajo el control judicial para pasar a depender de lo que determine el ordenamiento laboral (AGUSTINA SANLLEHÍ 2009).

Aunque superada, en su mayoría, esta visión, lo cierto es que los correos electrónicos, una vez descargados del servidor, leídos por su destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito del secreto de las comunicaciones (Sentencia del Tribunal Supremo de 17 de abril de 2013). Así, solo los no abiertos quedarían

dentro del ámbito de protección del art. 18.3 CE. Esto, trasladado al ámbito probatorio judicial, implica notables complicaciones, también apuntadas por los tribunales (Sentencia del Tribunal Supremo de 23 de octubre de 2018) pues habría de poder asegurarse, para justificar que no ha habido vulneración del secreto, que sólo se ha accedido a correos abiertos y que la herramienta informática utilizada impedía acceder a correos sin abrir, algo muy complejo de acreditar.

Habida cuenta de ello, y teniendo en consideración que el control del empresario respecto a los correos del trabajador suele producirse, con carácter general, *a posteriori*, esto es, una vez los correos se encuentran abiertos, en la práctica, el secreto de las comunicaciones suele quedar fuera del debate jurídico en pro del derecho a la intimidad del trabajador que sí opera ante ese compendio de correos abiertos y almacenados en el servidor (PINO PADRÓN 2018, p. 8).

En todo caso, la conclusión a la que hemos de llegar es que, para los correos electrónicos que están sin abrir, rige la protección que otorga el art. 18.3 CE, requiriéndose autorización judicial y, en cambio, para los mensajes abiertos, el derecho a la intimidad del art. 18.1 CE, que exige superar el test de proporcionalidad que veremos a continuación.

2.2.2. Derecho a la intimidad

Debido a la debilidad con la que opera el derecho expuesto en el apartado anterior, el control constitucional del correo del trabajador tiene que pasar, en la inmensa mayoría de casos, necesariamente, por el derecho a la intimidad. Así, el Tribunal Supremo, en su sentencia de 8 de febrero de 2018 recoge que "*el uso del correo electrónico por los trabajadores en el ámbito laboral queda dentro del ámbito de protección del derecho a la intimidad*".

Si revisamos el contenido esencial de este derecho, podemos identificarlo con la vida privada y, su protección, con la garantía de no sufrir intrusiones no deseadas en ella. Pero, ¿podemos tener vida privada en el trabajo? Y más concretamente, ¿hay algún espacio para hacer uso de la vida privada en el correo electrónico corporativo?

Con carácter general, el Tribunal Constitucional ha venido sosteniendo, en sentencias como la de 10 de julio del 2000, que el empresario no queda facultado para llevar a cabo, so pretexto de las facultades de vigilancia y control que le confiere el art. 20.3, intromisiones ilegítimas en

la intimidad de sus empleados en los centros de trabajo. Igualmente, el Tribunal Europeo de Derechos Humanos, en su sentencia de 3 de abril de 2007, en el famoso asunto *Copland*, determinó que los trabajadores conservaban su derecho a la intimidad aun cuando los dispositivos electrónicos fueran propiedad del empresario y su utilización se produjera durante el horario de trabajo. Así, consideró que los correos electrónicos remitidos desde el lugar de trabajo estaban protegidos en virtud del art. 8 del CEDH, relativo a la vida privada y familiar.

Algo muy positivo es que este reconocimiento general ha ido, en las últimas sentencias del Tribunal Europeo de Derechos Humanos, perfilándose en una línea más garantista. Fundamentalmente, se ha exigido un mayor nivel de información y transparencia en los controles del empresario al trabajador. No obstante, los criterios más recientes seguidos por la jurisprudencia del TEDH no aportan total certeza, debido, como han apuntado algunos autores, a la condición ulterior de nuestra normativa (DURO CARRIÓN, S., 2021, p. 85). Esto lleva a que convivan en una compleja relación dialéctica líneas jurisprudenciales nacionales menos garantistas con los nuevos criterios europeos.

El pronunciamiento judicial responsable de esta nueva corriente es el conocido caso *Barbulescu II*. Concretamente, la Gran Sala, para considerar que no hay vulneración de la intimidad del empleado, valora:

i) Primero, que el trabajador haya sido informado de forma clara y previa de la posibilidad de que la empresa adopte y aplique medidas de control.

ii) Segundo, el alcance del control y el grado de intrusión que implica en la vida del trabajador. En este punto, se tiene en cuenta el período de tiempo en el que se aplica la medida o el número de personas que tienen acceso a la información:

iii) Tercero, el motivo que ha proporcionado el empleador para justificar las medidas de control y su alcance. Cuando más invasiva sea esta supervisión, las razones legítimas alegadas deberán ser mayor peso.

iv) Cuarto, si existen otras medidas menos intrusivas para la privacidad de los trabajadores.

v) Quinto, el uso que haga la empresa de los resultados de la supervisión y las consecuencias que el control aplicado podría tener para el trabajador.

vi) Sexto, si las medidas de control han ido acompañadas de las correspondientes garantías para el trabajador, tales como la notificación previa o la información de la posibilidad de interponer una reclamación.

Vemos que, con esta nueva corriente jurisprudencial que abre Barbulescu II, en definitiva, se ha de pasar un primer test de transparencia, informando previamente al trabajador, después, un test de la finalidad, exigiendo un motivo legítimo para la intromisión y, por último, se debe aplicar el test de la proporcionalidad, primando los controles menos invasivos frente a que lo son más.

Además, dado que ya no es suficiente con que exista una prohibición de uso de los dispositivos digitales para fines privados, sino que es preciso informar al empleado de manera previa de la posibilidad de controlar sus comunicaciones, esta sentencia ha obligado a hacer una revisión necesaria de los criterios de los tribunales internos. Recordemos que lo que el propio Tribunal Supremo consideró en la Sentencia de 6 de octubre de 2011 - criticada por el desorbitado poder de control que otorgaba a los empresarios (TRUJILLO PONS 2016)- como meras "*obligaciones complementarias de transparencia*", ahora integra el contenido esencial del deber de información y, por ende, del derecho fundamental a la intimidad y al secreto de las comunicaciones (ROLDÁN MARTÍNEZ, 2017, p. 193). Así, sentencias como la del Tribunal Constitucional de 7 de octubre de 2013, que analiza la licitud de unos correos electrónicos obtenidos en el ordenador del trabajador, no pasarían el filtro garantista europeo. En esta sentencia, el Tribunal consideraba suficiente para anular la expectativa de privacidad la expresa prohibición en convenio del uso extralaboral del correo electrónico y su limitación a fines profesionales, pese a no existir una información previa por parte de la organización a los empleados, más clara, concisa y concreta. Lo relevante del caso, es que considera que si, en el convenio aplicable se tipifica como falta el uso privado de medios tecnológicos de la empresa, se considera legítimo el control empresarial sin necesidad de informar previamente al empleado. Como el trabajador debía conocer el convenio colectivo, no podía existir una expectativa fundada y razonable de privacidad.

Frente a los pronunciamientos previos a Barbulescu II, los posteriores han ido aplicando la nueva doctrina más garantista. Ejemplo de ello es la sentencia, también del Tribunal Supremo, de 8 de febrero de 2018, que declaró la procedencia del despido disciplinario de un trabajador con base en el control y examen de sus correos referentes a transferencias bancarias. En este

caso, el tribunal enumeró una serie de criterios muy similares a los del ya conocido como "test Barbulescu" y que, como no, recogen la necesidad de la información previa al trabajador respecto a la vigilancia de sus comunicaciones. Así, la sentencia establece los siguientes requisitos: i) el control de los correos electrónicos tiene que limitarse a contenido concreto; ii) el control debe referirse al correo profesional del empleado mediante el acceso al servidor alojado en las instalaciones de la empresa, no pudiendo accederse a ningún aparato o dispositivo particular del trabajador; iii) es conveniente y totalmente recomendable (que no obligatorio) que cuando el empleado accede con su ordenador a los sistemas informáticos de la empresa, de manera previa, acepte y consienta la Política de Seguridad de la Información, que deberá recoger que el acceso a este programa tiene fines estrictamente profesionales, reservándose la compañía el derecho a adoptar medidas de control para comprobar la correcta utilización; iii) informar expresamente al trabajador de la prohibición de utilizar el correo para fines particulares; iv) se recomienda que el empleador informe, previamente, de que puede controlar el cumplimiento de las directrices en el empleo de los dispositivos digitales.

2.2.2.1. Excepciones al deber de información previa

No obstante, es preciso tener en cuenta que, determinadas circunstancias pueden hacer que se module el test de proporcionalidad o, más concretamente, se flexibilice la valoración de alguno de sus criterios como el de la información previa al trabajador. De una revisión detallada de la jurisprudencia, destacan dos casuísticas en las que así ocurre:

a) Permisión de la vigilancia encubierta o control oculto o no transparente. En estos casos, la necesaria transparencia no se produce, pues el trabajador no es informado de las medidas de control. Se trata de un control excepcional, en el que no se informa al trabajador de manera anticipada, que la jurisprudencia parece aceptar bajo un patrón de riesgo de naturaleza, fundamentalmente, delictiva.

   En este caso, se ha venido considerando que la lógica de un control ordinario no debe ser aplicada del mismo modo cuando, más que una mera posibilidad, lo que hay es una sospecha fundada o patrón de riesgo de que el trabajador pueda estar incurriendo en una conducta tipificada penalmente (AGUSTINA SANLLEHÍ 2009).

Lo cierto es que existe jurisprudencia, como la sentencia del Caso Ribalda (Sentencia del TEDH de 9 de enero de 2018) que admite, ante la existencia de "sospechas razonables" de que se ha cometido un delito, el control encubierto. Y, aunque se refiere a la vulneración de la privacidad por una cámara oculta, no por el control y monitorización del correo electrónico, la doctrina considera que esta jurisprudencia puede extrapolarse también a los supuestos de control del correo electrónico (MONEREO PÉREZ, y ORTEGA LOZANO 2019, p. 141). A nivel interno, el Tribunal Constitucional, consideró en su sentencia de 10 de julio de 2000, con base en el mismo argumento, que las razonables sospechas de la comisión de graves irregularidades y la idoneidad de la medida de grabación para probar esas irregularidades, legitimaba las medidas de control establecidas. Igualmente, el Juzgado de lo Social nº 5 de Vigo de 30 de diciembre de 2022 consideraba superado el test de proporcionalidad debido a la concurrencia de un caso de competencia desleal. Este criterio también es usado por la jurisprudencia en el registro de las taquillas y los efectos personales del trabajador (CASAS BAAMONDE 2022, p. 3).

b) Hallazgos casuales. Otro de los supuestos que modulan el juicio de proporcionalidad y, especialmente, el deber de información al trabajador, es el de los hallazgos casuales. Este no sería sino un ejemplo fundado de sospechas, pero su fundamento se ha logrado concretar gracias a la sentencia del Tribunal Supremo de 8 febrero de 2018. En ella, el Tribunal confirmó la posibilidad de controlar el correo del trabajador por la existencia de pruebas documentales, validando que la empresa examinara los correos del empleado relativos a transferencias bancarias. En el caso, se tuvo en cuenta, además, que, en la Política de Seguridad de la Información, se señalaba que el acceso al correo lo era para fines estrictamente profesionales, reservándose la empresa el derecho de adoptar las medidas de vigilancia y control necesarias para comprobar la correcta utilización de las herramientas que ponía a disposición de sus empleados.

   Superado el test de proporcionalidad, es importante destacar que las evidencias obtenidas con estos controles son válidas, no anulándose en los procedimientos judiciales en los que se aportaron. Por ello, la doctrina sostiene que se excluye la aplicación de la doctrina anglosajona del "fruto del árbol envenenado", de tal forma que la prueba no se anula (MONEREO PÉREZ y ORTEGA LOZANO 2019, p. 154).

2.2.2.2. Anulación de la "expectativa de privacidad"

La jurisprudencia anterior, sin embargo, no otorga suficiente claridad sobre si es posible bloquear, con una prohibición expresa, la "expectativa de privacidad". Hay doctrina que considera que, efectivamente, cuando se implementen políticas de control sobre el uso del correo electrónico se puede reducir sustancialmente (SOUTO PRIETO y BOTANA LÓPEZ 2014), "*incluso eliminar por completo*" la expectativa de privacidad (AGUSTINA SANLLEHÍ 2009, p. 26). Otros, sin embargo, consideran que, incluso en el caso de que la empresa haya prohibido completamente el uso privado de los dispositivos puestos a disposición del empleado, "*ello no neutralizará plenamente toda expectativa razonable de privacidad"* (LUQUE PARRA y LACOMBA PÉREZ 2020, p. 379). Esta parte de la doctrina se apoya en la sentencia Barbulescu II que, en su párrafo 80, recoge que las directrices de una empresa no pueden anular el ejercicio de la "privacidad social" que todo trabajador tiene en su puesto.

Si por el contrario no se realiza una regulación expresa acerca del uso con fines extralaborales del correo electrónico, se deberá entender que el trabajador no está autorizado para el uso privado, aunque parte de la doctrina considera que el empleador debe tolerar un "uso razonable" del mismo conforme a la realidad vigente (AGUSTINA SANLLEHÍ 2009, p. 28). En estos casos, en los que no existe regulación por parte de la empresa, algunos han considerado que se parte de un reconocimiento tácito, por parte del empresario, del derecho a un uso social, concibiéndose esta conducta como inocua (CUADROS GARRIDO 2023, p. 704).

Ante esta situación jurisprudencial, la doctrina ha indicado que el principio de proporcionalidad al que recurren de manera constante las sentencias es, en definitiva, un principio "subjetivo" de la proporcionalidad, dado que la opinión del propio juzgador tendrá mucho que ver con el fallo final de la resolución judicial que, además, suele presentar votos particulares. En definitiva, la carencia de regulación legal al respecto, ha provocado una importante conflictividad jurisprudencial y el dictado de sentencias que ha terminado en todo tipo de consecuencias laborales (ORTEGA LOZANO y GUINDO MORALES 2020). Por ello, conviene hacer un llamamiento al legislador para la revisión de la normativa actual.

2.2.3. Derecho a la protección de datos

Aunque es desde la perspectiva del derecho fundamental a la intimidad, desde la que se ha tratado mayoritariamente la licitud o no del acceso al correo electrónico del trabajador, ello no es óbice para reconocer la afectación que estas prácticas tienen en el derecho fundamental a la protección de datos recogido en el art. 18.4 CE. La propia Agencia Española de Protección de Datos (en adelante, AEPD), en su conocido informe de 15 de noviembre de 2005 (reproducido por el Informe 0437/2010), reconoció sin resquicio a dudas, que la dirección de correo electrónico de los trabajadores era un dato personal, pues toda información asociada a esta dirección resulta identificable gracias a la misma. Por ello, el control del correo electrónico afecta de manera directa al derecho a la protección de datos del empleado.

Como es sabido, este derecho garantiza al ciudadano, y también, como no, al ciudadano que a su vez es trabajador, un poder de control o de disposición sobre el uso y el destino de sus datos personales, debiendo tenerse en cuenta, además, que los datos personales no son únicamente los datos íntimos, sino todos los datos que lo identifiquen o permitan su identificación. Es esta circunstancia la que determina que el ámbito de este derecho no coincida exactamente con la del del apartado primero del precepto constitucional, correspondiente al derecho a la intimidad.

Huelga decir en este punto que, aunque en el presente trabajo estamos revisando el control del empresario en las comunicaciones del trabajador para verificar si está desempeñando adecuadamente sus funciones laborales, el derecho a la protección de datos también ofrecería protección ante estas prácticas cuando el empresario tiene una finalidad distinta a la de controlar el desempeño del empleado. Por ejemplo, cuando el objetivo es cumplir una obligación legal como la de la desconexión digital para garantizar el respeto del tiempo de descansos y vacaciones. En estos casos, si el empresario no dispone de una alternativa menos invasiva, podría justificarse el acceso al correo electrónico (LUQUE PARRA y LACOMBA PÉREZ 2020, p. 364). Igualmente, el ámbito de la protección de datos también abarcaría las situaciones en las que el control del correo del trabajador se realiza con el fin de mantener la seguridad de la entidad. Es por ello que, instituciones garantes del derecho a la protección de datos, también se han pronunciado sobre estas casuísticas y han indicado que, de ser estrictamente necesarias estas medidas, el dispositivo debería configurarse de forma que evitara la captación constate de la actividad del trabajador o, en otro caso, no almacenara

datos de registro a menos que ocurra una incidencia (así lo recoge el GT29 en el Documento de trabajo de 29 de mayo de 2002, relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo indica que el control del correo electrónico del trabajador).

Sin embargo y pese a la amplitud de protección que este derecho puede proporcionar al trabajador frente a la potestad de control del empresario, los tribunales españoles están lejos asumirlo en este tipo de conflictos. Al contrario, vienen negando de facto la existencia en nuestro sistema jurídico de un principio de autodeterminación informática del empleado en controles empresariales. Como se indicaba, vienen localizando tan sólo los principios derivados de la intimidad y el secreto de las comunicaciones (ORTEGA LOZANO y GUINDO MORALES 2020). Por ello, desde la doctrina, y habiéndose detectado un uso abusivo de la intimidad para la resolución de estos conflictos, se está demandado la aplicación de la teoría de la "libertad informática" (PINO PADRÓN 2018, pág. 12) que, por el momento, no ha tenido reflejo en los pronunciamientos de jueces y magistrados.

Más allá de ello, sin embargo, el control del correo electrónico de un trabajador o de las aplicaciones que utilice para la comunicación dentro de la empresa constituye un tratamiento desde la perspectiva de protección de datos por lo que, a continuación, revisaremos los aspectos más relevantes del mismo.

2.2.3.1. La base legitimadora para el tratamiento de los datos personales derivados del control del trabajador

Aunque la atención que se ha prestado por parte de jueces y tribunales españoles al control de las comunicaciones del trabajador, desde la perspectiva de la protección de datos, ha sido cuanto menos escasa, no se puede negar que existe. En este ámbito, para que el tratamiento de los datos sea lícito, es preciso que exista una base jurídica que lo respalde. En el caso que estamos estudiando, de control para verificar el desempeño de las funciones de un trabajador, la base jurídica para llevar a cabo la supervisión del uso que éste hace de sus comunicaciones corporativas encajaría en el art. 6.1 b) RGPD. Este precepto legitima el tratamiento cuando éste es necesario para la ejecución de un contrato y resultaría aplicable al caso en tanto el tratamiento tiene lugar en el seno de una relación laboral.

En otros supuestos diferentes a los tratados en este trabajo, como el control para la verificación de la desconexión laboral, la supervisión del trabajador también podría tener cabida en el art. 6.1 c) RGPD, pues legitima el tratamiento cuando es necesario para cumplir una obligación legal exigible al responsable, en este caso, el empleador. Por otro lado, en el caso de que el empleador controlara el correo del empleado por motivos de seguridad IT, podría alegar el interés legítimo contemplado en el art. 6.1f RGPD, pues estaría protegiendo la red y los propios datos personales de los trabajadores y los clientes que se guardan en los servidores de la empresa, evitando accesos no autorizado o la fuga de datos. Pero, en todo caso, nunca encontraría el control del correo del trabajador su licitud en su consentimiento (art. 6.1.a) RGPD) toda vez que la relación empleador-trabajador se caracteriza por una desigualdad de poder entre ambos que podría condicionar y viciar el consentimiento prestado, en su caso, por el empleado, quien podría ofrecerlo por temor, principalmente, a perder su puesto de trabajo.

Como ya recogió el Comité de Ministros del Consejo de Europa en la Recomendación a los Estados miembros sobre el tratamiento de datos personales en el contexto del empleo, de 1 de abril de 2015, en su apartado 14.3 recoge que el acceso de los empresarios a las comunicaciones electrónicas profesionales de sus empleados debe darse una vez que estén previamente informados pero sólo puede producirse cuando sea necesario por motivos de seguridad u otros motivos legítimos.

2.2.3.2. Los principios de protección de datos aplicables al conflicto

La aplicación de la normativa de protección de datos a las medidas de control del correo electrónico del trabajador nos lleva al art. 5 del RGPD y, con él, a los principios que rigen la protección de datos y que aplican matices y añaden aspectos no contemplados en el "test Barbulescu II", propio del análisis desde la perspectiva del derecho a la intimidad (y no al derecho a la protección de datos) del trabajador.

De conformidad con el art. 5.1 a) RGPD, los datos deben ser tratados con licitud, aspecto que vendría salvaguardado por la base legitimadora antes indicada, y también con lealtad y transparencia. Esto último no es sino el derecho a la información previa que, como novedad, incluía la segunda sentencia de la Gran sala en el caso Barbulescu y que ya estaba recogida en

las normas de protección de datos vigentes (la entonces aplicable Directiva 95/46/CE lo recogía en su art. 10). Esta circunstancia no hace sino apuntar a que la normativa de protección de datos, que ha estado pasando desapercibida para los jueces que resolvían este tipo de conflictos, ya contenía una garantía que ha tardado años en llegar a asentarse en sede del derecho a la intimidad del art. 8 CEDH o 18.1 CE.

Igualmente, el apartado 5.1.b) RGPD, sobre el principio de limitación de la finalidad, recuerda a los criterios recogidos en el asunto Barbulescu II para valorar la existencia o no de proporcionalidad al caso concreto, exigiéndose que los datos sean recogidos con un motivo suficiente, esto es, (en el lenguaje propio de la protección de datos) con un fin determinado, explícito y legítimo.

Hasta aquí, estos dos principios (transparencia y finalidad) junto con el principio de minimización del art. 5.1c RGPD y su mandato de evitar el exceso de tratamiento de datos no estrictamente necesarios recuerdan a los criterios recogidos en el test de proporcionalidad. No obstante, el art. 5 RGPD ofrece una serie de principios que actúan como garantías adicionales y que no han sido expresados por la jurisprudencia al hilo de la resolución de los casos de supervisión de los dispositivos digitales puestos a disposición del trabajador. Hablamos del principio de exactitud, de la limitación del plazo de conservación o del principio de integridad y confidencialidad. Estos principios habrían igualmente de operar en las situaciones de control empresarial del correo del trabajador, otorgando una serie de derechos al empleado en los que, como decimos, los pronunciamientos judiciales, lamentablemente, no han puesto el foco.

El GT29, en su Dictamen 8/2001 avala la aplicación de estos principios, destacando que los datos recabados deben ser adecuados, pertinentes y no excesivos en relación con la finalidad, así como que los trabajadores han de ser suficientemente informados, destacando sobre la supervisión del correo electrónico profesional, que deberá ser proporcionada, teniendo en cuenta la privacidad de los empleados.

Aprovecharemos a tratar estas cuestiones en el apartado del presente trabajo "*Configuración de las medidas de control sobre los sistemas de comunicación corporativos*".

2.2.3.3. Los derechos que ostenta el trabajador derivados del Derecho a la protección de datos

La aplicación de la normativa sobre protección de datos otorga al trabajador objeto de control por parte del empresario una serie de derechos que, como se viene indicado, la jurisprudencia específica con la que contamos no ha recogido en modo alguno. Esto implica que un empleado tiene derecho de acceso a los datos que el empleador ha recogido a través de la medida de control de sus comunicaciones conforme al art. 15 RGPD y tiene derecho de rectificación, según lo indicado en el art. 16 RGPD, si hubiera alguna información incorrecta o incompleta. Tiene también derecho de supresión (art. 17 RGPD), de forma que podrá solicitar que los datos se supriman cuando estos ya no sean necesarios en relación con los fines para los que fueron recogidos, por ejemplo, cuando deje de prestar servicios en esa empresa o en ese puesto. Y aunque el derecho de oposición, por el tipo de base legitimadora no tiene aplicación directa a estos supuestos, el derecho recogido en el art. 22, relativo al derecho a no ser objeto de decisiones individuales automatizadas como la elaboración de perfiles podría tener aplicación si este tratamiento se está llevando por parte de la empresa.

2.3. Una oportunidad legislativa para abordar el conflicto: el art. 87 LOPDGDD

La afirmación que antes se hacía sobre la ausencia de normativa específica puede, *a priori*, sorprender ante un precepto incluido en la nueva LOPDGDD. Una de las novedades de esta ley fue la incorporación de su Título X, relativo a los derechos digitales. Entre ellos, se incluyó el art. 87 sobre el derecho a la intimidad y el uso de dispositivos digitales en el ámbito laboral. Esta hubiera sido una excelente oportunidad para regular de forma específica el poder de control del empresario frente a la intimidad del trabajador en el uso de los dispositivos digitales, pero, lejos de ello, el precepto no ha satisfecho estas expectativas. Algunos autores han apuntado a que su pretenciosa intención de regular el derecho a la intimidad y el uso de dispositivos digitales en el ámbito laboral no ha sido de gran ayuda. Su desafortunada redacción, como ha indicado DURO CARRIÓN (2011, p. 85), se limita a exponer el deber empresarial de información a los trabajadores sobre las normas que éstos han de cumplir en el uso de los dispositivos electrónicos puestos a su disposición.

Si revisamos el texto del artículo, comprobamos que la LOPDGDD reconoce, en su primer párrafo, que los trabajadores tienen derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por la empresa, aunque seguidamente, en su apartado dos, refleja el art. 20.3 del ET, reconociendo al empleador la posibilidad acceder a los contenidos derivados del uso de medios digitales. Después de "una de cal y una de arena", en su apartado tercero, determina que los empleadores deberán establecer criterios de utilización de los dispositivos digitales "*respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente*". No obstante, no es sino en el apartado *in fine* de este segundo párrafo, en el que el artículo menciona de manera más directa el control sobre los dispositivos electrónicos. Lo que parece entenderse de él es que, incluso en el caso de que se haya permitido el uso con fines privados, pueden realizarse controles, eso sí, previa información de los usos autorizados y previo establecimiento de las garantías precisas para preservar la intimidad de los trabajadores.

Esto que indica el precepto, llevado al ámbito del correo electrónico o las comunicaciones llevadas a través de aplicaciones de mensajería, deja numerosos interrogantes abiertos. Y es que, en el caso de que se permita el uso para fines privados del correo, si esta norma respalda el control empresarial de la cuenta, ¿qué tipo de garantías podrían establecerse para garantizar la privacidad de esos usos privados? Una de las opciones podría ser el filtrado de correos, por ejemplo, a aquellos que cuentan con la extensión empresarial, dejando fuera los que el empleado haya podido intercambiar con direcciones externas. Sin embargo, podría darse el caso de que el filtrado por correo y, en definitiva, por destinatario, no sea suficientemente garantista, pues puede haber conversaciones de carácter privado con miembros de la empresa.

Por otro lado, ¿qué ocurre cuando a pesar del mandato del art. 87.3 la empresa no ha regulado los usos de los dispositivos digitales? Estos casos no están previstos en el artículo pero, por la interpretación de conjunto, y dado que en la regulación siempre ha de haber lugar para un reducto de intimidad conforme a los usos sociales, entenderíamos que estaríamos ante una suerte de "silencio positivo". De esto también se deduce que no cabría una anulación completa de la expectativa de privacidad del trabajador, debiendo tener éste siempre intimidad conforme a los usos sociales. Huelga decir que este concepto jurídico indeterminado

de "usos sociales", por un lado, aporta flexibilidad de adaptación a la norma pero, por otro, genera determinada inseguridad jurídica, recayendo en los tribunales el peso de determinar qué se consideraría dentro y qué fuera. Lo que, entendemos, refiere una imposibilidad de anular completamente la expectativa de privacidad del trabajador. El GT29, que ya hablaba de la necesidad de que las políticas respetaran un uso "aceptable" en su Dictamen 2/2017, tampoco aporta mayor concreción al respecto. En este aspecto, habremos de esperar a que jueces y tribunales vayan formando criterios al respecto que puedan ir aportando luz a esta problemática.

Las primeras interpretaciones respecto a este precepto han sido dispares. Alguna voz del sector doctrinal ha venido a apuntar a que, si el primer párrafo reconoce el derecho a la intimidad de los empleados y el segundo la potestad de control del empresario, el tercero no es sino el procedimiento al que se tendrá que atender para que el control sea legítimo (LÓPEZ BALAGUER y RAMOS MORAGUES 2020, pág. 521). Desde esta perspectiva, si el uso de los dispositivos se ha limitado al ámbito exclusivamente profesional, la empresa deberá garantizar un respeto a la privacidad de acuerdo con los usos sociales. Si, por el contra, el uso para fines personales está permitido, el empresario deberá especificar de manera clara los usos autorizados y los períodos o momentos en los que pueden utilizarse para este ámbito privado.

El hecho de que esta interpretación sea "positiva" para el trabajador dado que incluso en la prohibición de uso para fines privados deja un resquicio de privacidad según los usos sociales (dentro de la ambigüedad que abandera), no hace que sea extensible a los tribunales. De hecho, la reciente sentencia del Tribunal Superior de Justicia de Madrid, de 4 de diciembre de 2023 (FJ II), señala que esta norma consagra legislativamente la doctrina del Tribunal Supremo, establecida desde la Sentencia de de 26 de septiembre de 2007, según la cual se puede neutralizar la expectativa razonable de confidencialidad del trabajador mediante la prohibición expresa del uso de los dispositivos digitales para usos privados y, a través de la información de que el contenido de los mismos podrá ser revisado por la empresa, con la finalidad de supervisión. En la misma línea argumentativa, se han pronunciado otras sentencias como la emitida por el Tribunal Superior de Justicia de Canarias el 8 de febrero de 2024.

En todo caso, lo que sí deja claro el precepto es que, para que el empresario pueda acceder a estos dispositivos, es necesario haber comunicado los criterios de utilización de las herramientas digitales, con indicación de las garantías para preservar la intimidad de los trabajadores. Así, "*Si no existen criterios de utilización del ordenador oportunamente comunicados a la empresa, difícilmente puede pretender que el uso privativo ha sido prohibido"* (FJ X, Sentencia Tribunal Superior de Justicia de Canarias de 21 de abril de 2023). Estos pronunciamientos, con terminología como la de la frase reproducida, no han detallado sin embargo qué tipo de "usos sociales privados" cabrían incluso dentro de esa prohibición.

Más al contrario, llevamos a ver sentencias en las que este aspecto se omite. Así, en la sentencia de la Audiencia Nacional de 22 de julio de 2022, el tribunal indicaba que, únicamente, en el caso en el que se permita el uso privado de los dispositivos, se requiere una previa especificación de modo preciso de los usos autorizados y el previo establecimiento de garantías para preservar la intimidad (FJ III). Por su parte, la Sentencia del Tribunal Superior de Justicia de Aragón de 13 de junio de 2022 recogía que el empresario debe establecer las pautas para el uso de medios informáticos y que sólo en el caso de que haya una prohibición absoluta de un uso personal de éstos, pueden implementarse controles.

Ante esta falta de claridad, y como habitualmente suele hacerse en Derecho para obtener luz en la interpretación de un texto legal, hemos acudido a su tramitación parlamentaria. En este caso, en la tramitación parlamentaria de la LOPDGDD, en la fase del Senado, se propuso una enmienda al art.87[i]. El Grupo Parlamentario Unidos Podemos- En Comú Podem- En Marea (GPPOD), formuló una enmienda al apartado segundo del artículo en el que incluía, después del reconocimiento del empleador para acceder a los contenidos derivados del uso de medios digitales, la especificación "relacionados con su actividad laboral" y, al final de la redacción actual, añadía otra finalidad, la de cumplir con las medidas de seguridad del RGPD. Este grupo parlamentario motivaba la enmienda indicando que es necesario diferenciar entre el acceso a los dispositivos en sentido amplio y el acceso a los contenidos específicos relacionados con la actividad laboral, a fin de que se pueda garantizar un espacio de privacidad para el trabajador. No obstante, esta enmienda no se aprobó, eliminándose este refuerzo de que siempre pueda existir contenidos no relacionados con la actividad laboral. No obstante, con la indicación en el art. 87.3 de que los criterios de utilización siempre han de respetar los usos sociales, podríamos entender salvaguardada la anulación completa de expectativa de privacidad. En

todo caso, no se registraron más enmiendas que puedan ayudar en la interpretación del precepto.

Por otro lado, debe apuntarse a que el art. 87 LOPDGDD hace una regulación del problema en este trabajo planteado, desde una perspectiva más propia del derecho a la intimidad del art. 18.1 CE que del derecho a la protección de datos pese a localizarse en la norma que desarrolla este derecho. De este modo, no recoge aspectos concretos del derecho a la protección de datos como los derechos de acceso que podría tener el trabajador o las obligaciones que el empresario adquiere. De hecho, en su dicción literal, podemos ver que hace referencia a la "intimidad", lo que, no obstante, bien podría entenderse en un sentido amplio que recoge todos los derechos contenidos en el art. 18 de la Carta Magna. Aún así, hubiera sido una buena oportunidad, más si cabe estando incluido en la ley reguladora de la protección de datos, incluir una mención a estos derechos del trabajador ante el tratamiento que haría la empresa si procede a controlar los dispositivos del empleado.

Precisamente, por esta configuración más propia del derecho a la intimidad, el art. 87, no excluye la existencia de que el control empresarial en los dispositivos del trabajador supere el test de proporcionalidad (FJ III; *Sentencia del Tribunal Superior de Justicia de Valladolid* 3 de marzo de 2022), recogiendo criterios del "test Barbulescu" como que no haya otro medio alternativo menos invasivo (JJ III, Sentencia del Tribunal Superior de Justicia de Galicia de 11 de noviembre de 2022).

Por último, es preciso añadir que, en 2021, otra ley podría haber abordado con mayor claridad la privacidad del trabajador en el uso de las herramientas que ofrece el empresario, precisamente, porque en este ámbito el control es más demandado por las organizaciones. Nos referimos al teletrabajo y su ley reguladora, la Ley 10/2021, de 9 de julio, de trabajo a distancia. No obstante, esta norma no ha establecido novedades al respecto. Su art. 17, además de remitirse a la LOPDGDD, reproduce prácticamente de manera literal lo recogido en el art. 87 de esta última. Y por su parte, el art. 22 de la Ley de trabajo a distancia repite el reconocimiento de la facultad de control del empleador, también por medios telemáticos, siempre respetando la dignidad del trabajador.

2.4. La posición de los organismos supranacionales de protección de datos

Aunque a nivel normativo no hemos logrado una regulación específica en este conflicto, instituciones relacionadas con la protección de datos, como el Grupo de Trabajo del Art. 29 sí se han pronunciado al respecto.

En el informe emitido en 2001, el GT29 recogía que "*Los trabajadores no dejan su derecho a la vida privada y a la protección de datos cada mañana a la puerta de su lugar de trabajo*", añadiendo que esperan legítimamente encontrar allí un grado de privacidad, ya que en él desarrollan parte importante de sus relaciones con los demás. Es llamativo que el GT29 llega a proponer que, para que el empleador pueda controlar la cuenta de correo electrónico del trabajador, sería conveniente que ofreciera dos cuentas al trabajador, una de uso profesional exclusivo y la otra de uso privado. Por otro lado, en su Dictamen 2/2017 sobre el tratamiento de datos en el Trabajo, reconociendo la posibilidad de control a través de medios informáticos, ha sido claro sosteniendo que debe garantizarse que los trabajadores puedan designar determinados espacios privados a los que el empresario no pueda tener acceso salvo en circunstancias excepcionales y, como principio, acoge la prevención a la detección. Así, si empresario desea impedir que el trabajador acceda a determinadas páginas ha de realizar el bloqueo, por lo que, a nivel de correo electrónico, si lo que se desea es, por ejemplo, evitar comunicaciones fuera de la organización, ha de bastar con capar la posibilidad de envío a dominios no corporativos.

Por su parte, a nivel interno, la AEPD, en su Informe 0615/2009, asume la posición del GT29, recogiendo que, en la medida de lo posible, la supervisión del correo electrónico debe circunscribirse a los datos sobre el tráfico de los participantes, siendo desproporcionado el acceso al contenido. Asimismo, indica que, salvo excepciones extremas como la vigilancia encubierta por tener sospechas de la comisión de un delito, el derecho de información debe cumplirse siempre.

En el ámbito internacional, la OIT, en el Repertorio de recomendaciones prácticas para la protección de datos de los trabajadores, no prohíbe la vigilancia de los trabajadores pero fija dos condiciones. Por un lado, que los trabajadores hayan sido previamente informados y, por otro, que el medio elegido ha de ser el más respetuoso para la vida privada de los trabajadores, no pudiendo elegir las empresas el que deseen. Además, su posición en cuanto a la vigilancia

secreta o permanente es muy restrictiva. Sobre la vigilancia permanente apunta a los perjudiciales efectos que tiene sobre la salud mental de los trabajadores, admitiéndola sólo en casos puntuales en los que sea necesaria para la saludado o seguridad y protección de los bienes. En el caso de la vigilancia secreta, sólo la admite cuando está contemplada por disposiciones de la legislación nacional, admitiéndola cuando existan sospechas razonablemente justificadas de actividades delictivas (apartado 6.14 de las Recomendaciones de la OIT sobre la protección de datos personales de los trabajadores).

Llama, en definitiva, la atención cómo estos organismos, años antes de la promulgación de nuestra LOPDGDD ya se han pronunciado con una claridad y definición mucho mayor que lo que lo ha hecho el art. 87. Pese a ello, entendemos que su existencia es un criterio interpretativo fundamental y su posición garantista una línea a seguir a nivel interno.

2.5. Nuevas formas de comunicación de la empresa: las aplicaciones de mensajería instantánea

Aunque la herramienta principal de comunicación interna, en empresas fundamentalmente digitales, sigue siendo el correo electrónico, como se indicaba desde el inicio, hay otras nuevas que cada vez están adquiriendo un papel más relevante. Hablamos, por ejemplo, de *Teams* de Microsoft o *Slack*. Se trata de *software* que permite la mensajería instantánea entre los compañeros de trabajo y que proporciona, a través de unas interfaces dinámicas, entornos de trabajo colaborativos funcionales y operativos.

Antes de revisar el funcionamiento de estas herramientas, es preciso destacar que el control de las mismas afecta a los mismos derechos ya estudiados en este trabajo. El hecho de que no estemos ante un servicio de correo electrónico no impide que estas aplicaciones, igual que aquel, permitan tener conversaciones privadas con otras personas (afectando al secreto de las comunicaciones), trasladar información atinente a la esfera privada (involucrando al secreto de las comunicaciones) o identificar a través del usuario registrado en las mismas al trabajador que hay detrás (concurriendo también el derecho a la protección de sus datos).

Habida cuenta de ello, vamos a adentrarnos en el funcionamiento de cada una de ellas con el fin de analizar qué retos, en el ámbito de la privacidad, plantean.

En el caso de *Microsoft Teams*, si accedemos a su página oficial, vemos que dispone de distintos planes empresariales. La propia Microsoft ofrece comparativas entre los mismos

para que el potencial cliente pueda decidir cuál se adapta mejor a su empresa. Si indagamos más, el propio equipo de Microsoft indica, en una respuesta a un usuario, que hay un informe para *Teams* que informa al administrador de cuánto tiempo pasa el trabajador en línea o ausente de la aplicación. Este "informe de actividad de usuario" se genera desde el "centro de administración" y permite exportar un archivo Excel en el que aparecerán los datos de todos los usuarios o trabajadores y que incluye el tiempo de audio, de video, de pantalla compartida y arroja datos sobre las tendencias de los últimos 7, 30, 90 o 180 días. Estos datos, sin embargo, se pueden configurar por la empresa como anónimos si así lo desea[1].

En el ANEXO A, se ha incluido la lista de informes sobre esta herramienta disponibles para el administrador que, en la organización, es el empresario con carácter general o, aquél que realice funciones de control y dirección en que éste delegue. Como se puede ver, hay una multiplicidad de informes que arrojan todo tipo de datos. Por ejemplo, en el "*Informe de uso de Teams*", el empresario puede ver el número de mensajes que cada trabajador ha publicado en un chat privado durante un período de tiempo concreto.

Ahora bien, no toda la información de la que provee la aplicación se limita a los citados informes. *Microsoft* cuenta con una herramienta llamada *eDiscovery*, incluida en el plan más costoso para empresas. Esta herramienta que se presenta como un mecanismo para ayudar con las investigaciones legales o permite almacenar de forma ordenada los mensajes intercambiados por la plantilla en caso de que sean relevantes para una investigación, permite también el acceso al contenido de las comunicaciones[2]. Tal y como se indica en la página oficial, eDiscovery otorga a la empresa la posibilidad de revisar y exportar conversaciones de los usuarios de *Teams* [3].

Otra herramienta habitualmente utilizada es *Slack*. Se trata de una de las aplicaciones más conocidas para la comunicación interna de las organizaciones. Esta herramienta diferencia entre mensajes privados y los que no lo son. Por ello, en su página web, informa de que los

[1] Información disponible en: https://learn.microsoft.com/es-es/microsoftteams/teams-analytics-and-reports/teams-reporting-reference
[2] Información disponible en: https://learn.microsoft.com/es-es/purview/ediscovery-teams-legal-hold
[3] Información disponible en: https://www.microsoft.com/es-es/security/business/risk-management/microsoft-purview-ediscovery

mensajes privados, directos entre uno o más usuarios, son "realmente" privados y aparecen en un grupo diferenciado de los canales abiertos[4].

Desde su panel de control de análisis de datos, todos los miembros de la aplicación pueden ver una serie de métricas que ofrece *Slack* (ANEXO C). Eso sí, la empresa advierte de que los datos de mensajes y archivos, canales y miembros sólo están disponibles con los planes de pago de *Slack*. Y, en todo caso, el análisis de los datos de canales cerrados sólo está disponible para un plan empresarial concreto, el plan Enterprise Grid y sólo para los propietarios y administradores con permiso para gestionar canales cerrados.

A estos efectos, si analizamos los planes que ofrece Slack comprobamos que son cuatro: uno gratuito, el "Pro", el "Business +" y el "Enterprise Grid"[5]. Sólo en estos dos últimos se incluye la funcionalidad "Exportaciones de datos para todos los mensajes". Esta herramienta permite exportar contenido de los canales, tanto públicos como privados, mensajes directos y todas las conversaciones de las que forma parte un usuario y dice expresamente "*según las necesidades y en la medida en la que permita la ley*". En este sentido, no se puede olvidar que *Slack*, perteneciente a la empresa SLACK TECNOLOGIES es una entidad estadounidense, donde la normativa de protección de datos se presenta más relajada.

Adicionalmente, *Slack*, en su página, incluye una "Guía para entender las herramientas de exportación e importación de *Slack*[6]. En ella, da una orientación de cuándo se van a poder requerir el contenido de los mensajes. Así, dice que sólo bajo determinadas condiciones, se podrán solicitar, indicando que las leyes laborales, de la privacidad o normativa interna de cada corporación puede limitar el uso de las exportaciones. Igualmente, indica que podría ser necesario que el empresario comunique al empleado que se va a realizar un acceso a sus conversaciones privadas.

No obstante, hay matices entre los distintos planes. En el "Gratuito" y en el "Plan Pro", las exportaciones son posibles bajo determinadas circunstancias. En estos casos, *Slack* pone a disposición un formulario para solicitar los canales y conversaciones, también los cerrados y

[4] Información disponible en: https://slack.com/intl/es-es/team-chat)
[5] Información disponible en: https://slack.com/intl/es-es/pricing
[6] Información disponible en: https://slack.com/intl/es-es/help/articles/204897248-Gu%C3%ADa-para-entender-las-herramientas-de-exportaci%C3%B3n-e-importaci%C3%B3n-de-Slack

los mensajes directos[7]. La aplicación advierte que sólo se aprobarán aquellas peticiones en las que se acredite un proceso legal válido, cuando se aporte el consentimiento de los miembros afectados o cuando se tenga potestad para ello de acuerdo con la normativa aplicable.

Sin embargo, en los otros dos planes, "Plan Business+" y "Plan Enterprise Grid" el funcionamiento es distinto. En ambos, se pone a disposición de la empresa una herramienta de autoservicio de exportación de datos, que incluye canales cerrados y mensajes directos, pero dice: según sea necesario y de acuerdo con las leyes aplicables. En estos casos, *Slack* señala que los propietarios de los espacios (las empresas) son los responsables de respetar la normativa, por lo que, en este plan, ya no es *Slack* quien acepta o rechaza una solicitud, sino la propia empresa quien debe determinar cuándo puede o no acceder a estos datos.

Es interesante citar alguno de los ejemplos que recoge la herramienta en los que*, a priori*, facilitará estas conversaciones privadas. En primer lugar, recoge el caso de que la empresa sea denunciada por acoso o, por ejemplo, robo de secretos comerciales. Otro de los casos es que el objeto social de la organización sean los servicios financieros y se vea obligada por ley a llevar registro de ciertas comunicaciones por un período concreto de tiempo. También se incluye el caso en el que un juez pueda ordenar que Slack aporte información a un procedimiento judicial para la investigación que corresponda. Y, por último, enuncia el supuesto en el que un antiguo trabajador solicite una copia de toda la información que se recoge sobre ella.

Como se ha podido comprobar, los proveedores de programas empresariales para la comunicación interna ofrecen métricas en cuanto al número de correos y acciones, pero en ellos, en primer término, no se revelan elementos de la comunicación tan relevantes como lo pueden ser el destinatario y el propio contenido de la comunicación. Es más, permiten incluso la posibilidad de hacer inidentificable al usuario. Ello no obsta a que, como ocurre en el caso de *Slack*, cuando concurra una razón legítima o consentimiento del trabajador, el empresario pueda solicitar el contenido de las conversaciones a la empresa proveedor. Sin embargo, como se ha visto en ambas herramientas, la empresa puede contar con herramientas para acceder directamente al contenido de las conversaciones cuando el plan que haya contratado lo

[7] Información disponible en: https://slack.com/intl/es-es/help/requests/new

permita. Esta opción puede resultar arriesgada pues puede otorgar, *a priori*, una información excesiva a la que, ha de ser la empresa quien, autorestringiéndose, no acceda. De lo contrario, es claro que podrían conculcarse los derechos al secreto de las comunicaciones, a la intimidad y a la protección de datos del trabajador, procediéndose, en caso de que con ellos se haya obtenido una evidencia aportada como prueba en un procedimiento contencioso, a anularse la misma.

En todo caso, puede notarse cómo el planteamiento de estas aplicaciones es, a nivel técnico, recoger todas las funciones posibles (pues su mercado es internacional y las necesidades y posibilidades dentro del marco legal aplicable a cada empresa pueden ser diferentes) y, a partir de ahí, acomodar sus funcionalidades o servicios a lo que requiera el cliente, esto es, la empresa contratante, a través de los distintos planes que ofertan. Esto, a juicio personal, incurre en cierta contradicción con los principios *privacy by design and default* que vertebran el Reglamento de Protección de Datos Europeo y que, proviene, en definitiva, de que el desarrollo de estas aplicaciones está fuera del panorama europeo.

2.6. Vías de control del correo electrónico del trabajador: especial referencia a la monitorización

El hecho, por un lado, de que el correo electrónico o las aplicaciones de mensajería corporativa se distribuyan por un proveedor de servicios y, por otro, que el trabajador las utilice desde un dispositivo entregado por la empresa, hace que haya multiplicidad de posibilidades para acceder al uso que se hace de las mismas. A grandes rasgos, la utilización de estas herramientas por el empleado puede controlarse de cuatro formas.

La primera consiste en el acceso directo al equipo o, en su caso, a los servidores propios donde se almacenen los datos. Otra de las opciones, es mediante la solicitud de datos a los proveedores de las aplicaciones de mensajería, tal y como hemos visto en el apartado anterior. Es este sentido, es preciso indicar que, también es posible obtener esta información de los proveedores de correo electrónico. De hecho, *Microsoft*, al igual que hace con *Teams*, también ofrece al administrador información sobre la actividad del email. Según puede verse en el ANEXO B, los informes que facilita muestran, entre otras cosas, cuándo el trabajador realizó una actividad de lectura o envío de correo, el número de veces que registró una acción de

envío, esto es, cuantos correos ha remitido o cuantas veces registró una acción de lectura, es decir, cuantos correos ha leído. Y, también, *eDiscovery* ofrece información sobre los correos, teniendo en este aspecto, un régimen similar al de las aplicaciones de mensajería.

Además de estas vías de control, otra, aunque no tan habitual, podría darse mediante la instalación de un sistema de vigilancia, siempre que una de las cámaras enfoque a la pantalla del trabajador. Este mecanismo, sin embargo, no resulta de utilidad cuando la modalidad es el teletrabajo. Aunque el objeto de este trabajo no es la videovigilancia en el ámbito laboral, lo cierto es que una cámara de videovigilancia orientada hacia el ordenador de un empleado puede captar toda su actividad en el equipo, y por qué no, el uso que el trabajador haga del correo electrónico o de otras aplicaciones de mensajería de la organización, pudiendo incluso captar el contenido de los mensajes remitidos o enviados.

Aunque a nivel técnico ello es posible, es importante indicar que, *a priori*, estas prácticas no se encuentran amparadas en Derecho. En este ámbito, debemos nombrar la conocida Sentencia del Juzgado núm. 2 de Badajoz que considera que el enfoque de la cámara de videovigilancia a la pantalla del ordenador es una vulneración del derecho a la intimidad y a la propia imagen. El juez considera que no supera el juicio de idoneidad, necesidad y proporcionalidad porque el Ayuntamiento (dado que se trataba de una empleada pública) no justificó de manera razonable la concreta ubicación y orientación de la cámara. De hecho, la sentencia afirma que la cámara proporciona un control continuado de la actividad de la trabajadora sin justificación. Es interesante, además, saber que la sentencia considera que el derecho a la igualdad queda vulnerado, porque existiendo solo dos cámaras una enfoca solo a esta trabajadora.

Por último, una de las formas más utilizadas en la actualidad para controlar el uso de los dispositivos digitales por parte de los empleados es la instalación de un *software* de monitorización que, entre otras funciones puede controlar las comunicaciones del trabajador.

La mención a este tipo de sistemas es, sin embargo, necesaria pues, a partir de la pandemia y de la llegada del teletrabajo y a pesar de lo intrusivos que puedan resultar, se han desarrollado programas de *software* que son capaces de monitorizar toda la actividad del trabajador en su equipo. Estos programas son capaces de controlar qué hace el trabajador en cada momento mediante la toma de capturas de la pantalla, el control de las pulsaciones en el teclado, los

accesos a páginas de Internet o redes sociales e, incluso, activar la cámara del equipo pudiendo obtener información de si el empleado se encuentra sentado o si se ha ausentado.

Todas estas funcionalidades tienen implicaciones en la intimidad del trabajador, incluso, en algunos casos, en su derecho a la propia imagen. No obstante, siendo el objeto de este trabajo el control del correo del trabajador, nos centraremos especialmente, en este punto.

A este respecto, es evidente que un programa que tome capturas de pantalla aleatorias o, incluso, realice una grabación constante, va a captar las conversaciones que mantenga el trabajador, ya sea en el correo electrónico, ya en otras aplicaciones de mensajería como que utilice la empresa, como puede ser *Teams*.

En todo caso, y bajo criterio personal, la clave para determinar la adecuación a Derecho de estas herramientas es determinar si lo que se va a captar se puede recoger. Así, si no se puede captar el contenido de las conversaciones de los trabajadores, ni una videocámara enfocada al ordenador ni un acceso al equipo ni tampoco un sistema de monitorización que tome capturas o grabe la pantalla va a considerarse legal. De este modo, lo relevante del medio o vía de acceso que se emplee es que, dependiendo de cuál se implemente, puede recoger datos de una manera más o menos indiscriminada y, en el caso de la monitorización, puede ser una forma, como se decía, extraordinariamente intrusiva.

Con carácter general, diremos que una captación constante de la pantalla del ordenador de un trabajador no podría superar el test de proporcionalidad analizado en los primeros apartados del trabajo. Estos programas, habitualmente, son invisibles para el trabajador, no apareciendo ningún icono en su escritorio o ni ninguna evidencia de ellos en el listado de programas instalados en el equipo. Pero, incluso en el caso de que estas medidas de control se informen a los trabajadores, así como su alcance y consecuencias, es presumible pensar que hay medidas menos intrusivas para supervisar el correcto despeño por un trabajador de sus tareas laborales. De esta forma, no pasaría el "Test Barbulescu" asentado desde el análisis de la vulneración del derecho a la intimidad del art. 18.1 CE. Tampoco, por otro lado, podría entenderse respetado el principio a la minimización de datos, considerándose, por tanto, vulnerado el derecho a la protección de datos, contemplada en el art. 18.4 CE del trabajador. Igualmente, a la luz de los criterios de la AEPD y del GT29 vistos en apartados anterior, estas herramientas podrían considerarse válidas.

Sin perjuicio de ello, cuando la monitorización no se lleve a cabo con todas las funcionalidades descritas, por ejemplo, excluyendo la toma de capturas de pantalla periódica, la valoración puede ser otra. Por ello, vamos a ver alguno de los programas que existen en el mercado, qué funciones tienen y cómo operan.

Uno de los más conocidos es *CleverControl*. Este *software*, desarrollado por una empresa de Florida, permite, entre otras funciones, supervisar la actividad de correo electrónico corporativo de los empleados. Es cierto, no obstante que, como ocurría en el caso de las aplicaciones de mensajería instantánea corporativa, volvemos a ver una descarga de responsabilidad en la empresa compradora de este *software*. En la página web, la empresa indica que es necesario que el empresario se cerciore de que tiene derecho a controlar la actividad del correo electrónico de los trabajadores, recordando que debe tener en cuenta las leyes y reglamentos que rigen la privacidad del correo electrónico[8]. La propia empresa hace referencia al RGPD e indica que el Reglamento no trata de manera concreta el control de los trabajadores a través de la vigilancia de su ordenador, de su correo electrónico o de sus redes sociales, llamando la atención que anime por ello a recabar el consentimiento de los empleados y que indique que el Reglamento impide que se lleve a cabo registro de pulsaciones del teclado o capturas de la pantalla del trabajador[9]. Sobre lo primero, consideramos que el consentimiento, como ya se ha dicho, no es una base legitimadora válida en la relación laboral. Y sobre lo segundo, ciertamente, el GT29 ha considerado que el tratamiento que implican estas tecnologías es desproporcionado (p. 17, WP 249, Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, de 8 de junio), pero, al contrario de lo que se da a entender, el RGPD, expresamente, no señala nada al respecto.

En el caso de *Spyrix Employee Monitoring*, herramienta desarrollada en California, se repite el mismo patrón. En su página web vemos que, al final de la interfaz inicial, aparece una nota legal en la que se indica que es una violación de las leyes federales y estatales de Estados Unidos la instalación de este programa en un equipo para el que no se dispone de

[8] Información disponible en: https://clevercontrol.com/es/best-employee-monitoring-software
[9] Información disponible en: https://clevercontrol.com/es/control-de-los-empleados/

autorización, y, empresas radicadas fuera de Estados Unidos, recomienda consultar su legalidad en el Estado en el que se vaya a utilizar[10].

No obstante, hay programas de monitorización que difieren de los expuestos. Por ejemplo, el software ActivTrak, también americano, indica en su página web que mide la productividad pero protegiendo la actividad de los empleados, añadiendo que no registra pulsaciones de teclas, no accede a la cámara, no monitorea dispositivos electrónicos y no controla el correo electrónico[11]. Esta herramienta, además, indica cómo configurarla para el cumplimiento del RGPD. Y cuenta con herramientas para proceder a la eliminación de usuarios cuando corresponda la supresión, permite correcciones de información, permite eliminar todos los datos asociados a un empleado y permite compartir los datos con el personal a través de un portal de forma que se pueda dar acceso a los empleados[12].

En el ámbito español, entre varias, encontramos la herramienta desarrollada por LINKA Ciberseguridad Gestionada. Se trata de una aplicación que también cuenta con software de control de empleados[13]. Una de sus funcionalidades es la de monitorizar la pantalla de los empleados a tiempo real, registrar las pulsaciones del teclado y, dice, "*muestra los correos recibidos y enviados por los empleados*". También revela conversaciones de chats entrantes y salientes. Además, dice que es completamente legal en España, al haber sido desarrollada por juristas especializados en la materia. Sin embargo, como se ha indicado más arribas, a juicio personal, este tipo de funcionalidades plantean serias dudas por lo intrusivas que pueden resultar para la privacidad del trabajador.

2.7. Configuración de las medidas de control sobre los sistemas de comunicación corporativos

Una vez determinadas las normas aplicables a la imposición de medidas de control al correo corporativo del trabajador, y teniendo en cuenta las peculiaridades de los sistemas de control

[10] Información disponible en: https://www.spyrix.com/es/employee-monitoring.php
[11] Información disponible en: https://www.activtrak.com/
[12] Información disponible en: https://support.activtrak.com/hc/en-us/articles/10220131064731-How-to-Configure-ActivTrak-for-GDPR-Compliance
[13] Información disponible en: https://www.grupolinka.com/control-ordenadores-empleados/#

existentes, conviene determinar qué pasos debe dar la empresa para que sus mecanismos de supervisión sean legales, qué proceso se debe seguir para adoptarlos y cómo configurarlos correctamente.

2.7.1. Definición del control a llevar a cabo.

El empleador, en primer término, ha de decidir el tipo de datos a los que desea acceder y, por tanto, qué alcance van a tener las medidas de control. En este punto, es preciso que el motivo que lleva a tomar la decisión de implementar controles esté suficientemente justificado, teniendo estos controles, como indican los arts. 20.3 ET y 87 LOPDGDD, que estar orientados a supervisar el cumplimiento de las obligaciones y deberes laborales del empleado.

Pero, el hecho de que la empresa cuente con un motivo justificado no es suficiente. Es importante distinguir entre el derecho del empleador a implementar controles y si el modo de llevarlo a cabo y el uso de sus resultados son adecuados (Sentencia del Tribunal Superior de Justicia de Cataluña de 20 de abril de 2022).

Por eso, en este primer momento, la empresa también debe definir la medida de control así como el medio para llevar a cabo esta vigilancia teniendo en cuenta los principios de proporcionalidad y minimización de datos. Y, si para el fin perseguido, existen medidas menos intrusivas, optar por éstas. Así, si la empresa quiere limitar el uso del correo electrónico a usuarios internos, antes de acceder a los mensajes, podría bloquear el envío de correos a direcciones de correo que no tuvieran la extensión de la empresa. En este sentido, el GT29 ha dicho que, para cumplir el requisito de subsidiariedad, es preferible antes de controlar las comunicaciones, optar por el bloqueo (Documento de trabajo de 29 de mayo de 2002, relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo). Igualmente, antes de acceder a la totalidad correos y a su contenido, filtrar por destinatario, fecha o asunto, de forma que se acceda a los que sean estrictamente necesarios.

Por otro lado, en la medida de lo posible, será conveniente acceder al correo a través del servidor y no a través del ordenador (Sentencia del Tribunal Supremo, de 8 de febrero de 2018).

2.7.2. Valoración del impacto en la privacidad (la EIPD).

Definida ya la medida de control a implementar, en esta fase, se deben analizar los riesgos que genera para la privacidad de los trabajadores. Para ello, es preciso tener en cuenta a qué datos se accede (sólo al número de correos enviados, a la fecha y hora de las comunicaciones, a los destinatarios, etc.) y durante cuánto tiempo la supervisión.

En caso de que se vaya a suscribir un plan empresarial con una herramienta como *Teams*, será preciso consultar con el Delegado de Protección de Datos o, si la empresa no cuenta con éste, con un servicio de asesoría jurídica si las funcionalidades contratadas son acordes a Derecho.

Si, además, se va a optar por implementar un *software* de monitorización del dispositivo del empleado, será preciso realizar una evaluación de impacto o EIPD, como ya apuntaba el GT29 en su Dictamen 2/2017. Siguiendo lo indicado en el art. 35 RGPD, es precisa su realización para los casos en los que sea probable que un tipo de tratamiento, especialmente si utiliza nuevas tecnologías, entrañe un riesgo alto para los derechos y libertades de las personas físicas. Además, si acudimos a la Lista que ofrece la AEPD, uno de los tratamientos recogidos y que, por ende, requiere de la realización de una EIPD es aquel que implique la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva. No cabe duda, a estos efectos, de que un *software* que está operativo de manera constante mientras el trabajador usa el equipo es una observación sistemática.

En la evaluación, la empresa deberá realizar un análisis de necesidad y proporcionalidad del tratamiento. Y también, se deberán identificar las amenazas y los riesgos, evaluar el riesgo inherente y, una vez adoptadas las medidas oportunas, el riesgo residual.

2.7.3. Adopción de garantías: registro de accesos

Tanto la regulación de la EIPD, como el art. 87 LOPDGDD y la jurisprudencia que hemos visto, en especial, Barbulescu II, recogen la necesidad de implementar garantías para salvaguardar la privacidad de los trabajadores. Una posible medida a tener en cuenta en la supervisión del correo electrónico es la recogida en el art. 103 del RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Esta norma, que sigue estando vigente y sirve de orientación para determinar las medidas de seguridad a adoptar dependiendo del nivel de

riesgo, recoge, como garantía para un nivel alto, el registro de accesos bajo el control directo del responsable de seguridad. Esto se antoja necesario en los sistemas de supervisión de las comunicaciones del empleado.

2.7.4. Aprobación de los criterios de utilización de los dispositivos digitales: participación de los representantes de los trabajadores

Determinada la medida, valorado su impacto en la privacidad de los trabajadores y adoptadas las medidas de seguridad necesarias, para que su aprobación sea válida, es imprescindible que, en ella, participen los representantes de los trabajadores. Aunque a ello ya se apuntaba por instituciones como el Comité de Ministros del Consejo de Europa (en la Recomendación a los Estados miembros sobre el tratamiento de datos personales en el contexto del empleo, de 1 de abril de 2015), el marco jurídico actual lo ha positivizado de manera expresa. En este sentido, el art. 64 ET establece que el comité de empresa tiene derecho a ser informado y a emitir informe, con carácter previo a que el empresario ponga en marcha, entre otros, sistemas de organización y control del trabajo. Así lo ha reconocido también ampliamente la doctrina (POQUET CATALÁ, 2018).

A su vez, el apartado tercero del artículo 87 LOPDGDD, en consonancia con el art. 88 RGPD y con el citado 64 ET, encomienda, como hemos visto, a los empleadores el establecimiento de unos criterios de utilización de dispositivos digitales, recogiendo de nuevo la necesidad de que participen los representantes de los trabajadores.

Por ello, una de las vías más utilizadas para implementar estos controles ha sido la de su inclusión en el convenio colectivo aplicable. En todo caso, es importante tener en cuenta que recoger estos controles en el convenio no excluye el deber de información a los trabajadores, tal y como ha recogido la jurisprudencia más antigua (por ejemplo, el Tribunal Constitucional en sentencia de 22 de febrero de 2013) y la jurisprudencia recaída a partir de Barlubescu II,.

2.7.5. Aprobación de los criterios de utilización de los dispositivos digitales: contenido mínimo de privacidad conforme a los usos sociales

Además del requisito procedimental consistente en que participen los representantes de los trabajadores, el art. 87 LOPDGDD impone una limitación material, al indicar que los criterios de utilización de los dispositivos deberán respetar unos estándares mínimos de protección de intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. Esto nos lleva a afirmar que, las políticas que prohíban completamente la utilización de los dispositivos digitales para efectuar comunicaciones privadas no son legales.

2.7.6. Deber de información a los empleados

Sin perjuicio de que se cumplan todos los pasos anteriores, es imprescindible informar de manera detallada y precisa a los trabajadores, primero, de la decisión de supervisar su correo o los programas de mensajería empresariales y, segundo, de cuestiones como la forma en la que se va a hacer (por ejemplo, a través de un *software* de monitorización), el período de tiempo al que la supervisión se va a circunscribir o las consecuencias que puede tener un uso inadecuado o no contemplado en los criterios de uso a los que alude el art. 87 LOPDGDD.

Además, la empresa deberá informar al trabajador conforme al art. 11 y 13 de la LOPDGDD y del RGPD, respectivamente. De esta forma, el empresario deberá informar a los trabajadores: de los datos de contacto del delegado de protección de datos, si lo hubiera; de los fines del tratamiento a los que va a destinar los datos que, en este caso, serán la supervisión de la actividad laboral y el control del rendimiento. También deberá incluir la base jurídica del tratamiento, en la que se encuentra excluido el consentimiento a razón del desequilibrio entre empresario-trabajador. Así, habitualmente, la base jurídica es la ejecución de un contrato y los intereses legítimos, toda vez que haya proporcionalidad y subsidiariedad. Esta información también deberá incluir los destinatarios o las categorías de destinatarios o la intención de transferir los datos a un tercer país u organización internacional. Esto último puede ser común dado que muchas de las aplicaciones de monitorización se encuentran radicadas en el extranjero. Y, tal y como se indica en el art. 13.2 RGPD, se deberá informar al trabajador del plazo por el que se conservarán los datos y, como no, si se van a utilizar para adoptar decisiones automatizadas.

Como indica el art. 13.2 RGPD , también es preciso informar a los trabajadores de los derechos que les asisten en cuanto al acceso, la rectificación o supresión de los datos, así como la posibilidad de plantear reclamaciones ante la autoridad de control. Para ello, la empresa debe contar con un procedimiento habilitado para encauzar el ejercicio de estos derechos por parte de la plantilla de personal. En caso contrario, esta denegación podrá ser impugnable (así se ha recogido, desde instancias europeas, en el Manual de legislación europea en materia de la protección de datos).

2.8. IMPLICACIONES DEL USO INAPROPIADO DE LOS MECANISMOS DE CONTROL

En el último apartado de este trabajo, se desea hacer una somera mención a las consecuencias que puede tener para el empleador la inadvertencia de los requisitos y obligaciones que hemos analizado y que deben concurrir para la adecuada implementación de medidas de control del correo electrónico del trabajador.

La primera consecuencia del uso inapropiado de los mecanismos de control por parte del empleador es la ilicitud de la prueba en los procedimientos judiciales que se hubieran podido iniciar. La propia Ley Orgánica del Poder Judicial establece que, en todo procedimiento, se respetarán las reglas de la buena fe, no surtiendo efecto las pruebas obtenidas, directa o indirectamente, vulnerando los derechos o libertades fundamentales (art.11.1 LOPJ).

En todo caso, el efecto práctico de la ilicitud de la prueba, habida cuenta de que, habitualmente, se aporta por el empleador en el proceso judicial con el objetivo de ratificar un despido disciplinario por transgredir la buena fe contractual, es el mantenimiento del trabajador en la plantilla.

Fuera de las salas de lo social, la supervisión del correo del trabajador al margen de los requisitos legales puede lugar a otro tipo de responsabilidades. Por un lado, las acusaciones que hubiera podido interponer la empresa con base en las evidencias captadas a través de esta supervisión (por ejemplo, para imputar un delito por competencia desleal a un empleado) quedarían archivadas. Por otro, en otros casos, el propio en empleador podría incurrir en el delito tipificado en el art. 197 del Código Penal, correspondiente al descubrimiento y revelación de secretos. No obstante, tiene que resultar acreditado que el objeto del empleador es vulnerar la intimidad del trabajador y no la de controlar su desempeño laboral.

Por ello, se ha apuntado a que, en la práctica, es complicado que este tipo penal pueda resultar aplicable en la medida en que el empresario no realizar el control del correo "para" vulnerar la intimidad del trabajador (ROLDÁN MARTÍNEZ 2017). Cuando ello ocurre, normalmente, es una "consecuencia colateral" al objetivo de control de las funciones laborales del empleado. También debe tenerse en cuenta que realizar una supervisión específica de un trabajador y del al resto de la plantilla podría poner sobre la mesa el delito de acoso 173.1 del Código Penal. No obstante, además, sería preciso que concurrieran las notas definitorias del tipo.

En todo caso, el inconveniente que se ha presentado en la práctica es que no todos los órdenes jurisdiccionales han procedido del mismo modo respecto a la prueba. En el ámbito penal, y para el caso de las comunicaciones en curso, el Tribunal Supremo aclaró, en su sentencia de 16 de junio de 2014, que la doctrina contenida en las sentencias de lo social, no aplica al ámbito penal, donde se exige la autorización previa para intervenir las comunicaciones por imperativo del art. 18.3 de la Constitución.

Por último, es necesario mencionar que el empresario está sometido a las multas económicas que recoge el RGPD en su art. 83. Así, cuando no se respeten alguno de los principios contenidos en el art. 5 RGPD, el deber de información del art. 13 o cualquiera de los derechos que ostenta el trabajador, como el derecho de acceso, la empresa puede ser sancionada con multas administrativas de hasta 20.000.000 euros o de hasta el 4 por ciento de su volumen de negocio total anual global.

De esta forma, el ordenamiento jurídico cuenta con mecanismos suficientes para incentivar a las organizaciones a cumplir con la normativa aplicable y, de esta forma, garantizar la privacidad del trabajador en el uso de los dispositivos digitales que le han sido ofrecidos y, como no, en el empleo de las comunicaciones electrónicas en el entorno empresarial.

3. Conclusiones

Del presente estudio sobre el conflicto entre el poder de control del empresario y la privacidad del trabajador en el uso del correo electrónico, se han podido llegar a las siguientes conclusiones:

Primera.- Se puede concluir que la jurisprudencia europea presenta una posición más garantista respecto a la intimidad del trabajador que la jurisprudencia interna. Este contraste requiere de la actualización en los criterios que jueces y magistrados han de emplear cada día

en sus resoluciones, debiendo acogerse como eje vertebrador el principio de información al trabajador de cualquier medida de control que se le vaya a aplicar.

Segunda.- A pesar de que instituciones reconocidas en materia de protección de datos vienen, desde hace años, reconociendo el derecho a la autodeterminación informativa del trabajador, ni el TEDH ni los tribunales españoles han incorporado en su cuerpo jurisprudencial este derecho y todas las facultades que de él derivan. En este ámbito, será necesaria una labor progresiva de integración de esta normativa junto con los criterios ya existentes para valorar la intromisión en el derecho a la intimidad.

Tercera.- En consonancia con lo anterior, se muestra necesaria una propuesta legislativa concreta que recoja el derecho a la protección de datos del trabajador, no resultando suficiente el avance contenido protagonizado por la incorporación del art. 87 LOPDGDD, artículo que no ha conseguido delimitar en detalle los límites al poder de control del empleador.

Cuarta.- La jurisprudencia y su manido recurso al test de proporcionalidad siguen dejando interrogantes abiertos, especialmente, en relación a los sistemas de monitorización de las comunicaciones. Este test de proporcionalidad, en el ámbito de la protección de datos, puede integrarse en una evaluación de impacto (EIPD) que determine si el tratamiento es necesario para lograr un fin legítimo, incluyendo las medidas que garanticen la mínima injerencia en la intimidad y el secreto de las comunicaciones de los trabajadores.

Quinta.- Las aplicaciones de *software* para el control de la actividad del trabajador, fundamentalmente desarrolladas fuera del entorno europeo, no están creadas desde el principio del *privacy by design*, debiendo las empresas que opten por ellas, realizar una evaluación previa de adecuación a nuestra normativa que, en la mayoría de casos, requerirá limitar las funciones de control, por ejemplo, excluyéndose las capturas de pantalla períodicas de la pantalla del ordenador.

Octava.- El fuerte incremento de las aplicaciones de mensajería instantánea dentro de las empresas hace necesaria la aplicación de los criterios existentes ya orientados al control del correo electrónico a estas nuevas herramientas, requiriendo de la adopción, por parte de las empresas, de políticas internas de uso de los dispositivos y herramientas de trabajo cada vez más detalladas y precisas a fin de poder conseguir la seguridad jurídica que, a día de hoy, ni

los variados pronunciamientos jurisprudenciales ni las lagunas jurídicas que sigue habiendo en la legislación, han permitido.

4. Opinión personal del autor

Sin ánimo de que esta opinión personal sea un "voto particular" *sui generis* de las conclusiones alcanzadas, sí que aprovecho este espacio para aportar mi propia visión del conflicto y que, considero, cada vez se aproxima más al camino que Europa está marcando en la cuestión.

A nivel personal, considero que un equipo informático es un "mecanismo de producción" que la empresa pone a disposición del trabajador. Por extensión, lo mismo ocurre con una dirección de correo corporativo que habitualmente se crea para el empleado al ingresar a la empresa o su perfil de *Teams* o cualquier herramienta corporativa. No obstante, estos mecanismos de producción tienen matices muy relevantes respecto los mecanismos de producción tradicional. En mi opinión, no solo los considero una herramienta de trabajo cuyo control empresarial sea incuestionable o ilimitable, como una máquina para empaquetar, sino todo un entorno empresarial, una especie de ecosistema completo de trabajo. En una empresa tradicional alejada del entorno digital, una máquina de empaquetado era una herramienta más de trabajo a todas las que prestaba la empresa. Ahora, un ordenador, puede ser única y exclusivamente, la empresa completa.

Al punto al que deseo llegar es que, en un trabajo, ajeno al mundo digital, el empleado puede disponer de una máquina para, como hemos dicho, empaquetar un producto, pero también dispone de una taquilla personal. Esta taquilla personal no se puede registrar pues para ella opera el límite de registro que el art. 18 del ET. Igualmente, puede tener conversaciones con sus compañeros en un pasillo de la empresa que no pueden ser captadas por un sistema de videovigilancia de sonido y que, lógicamente, pueden ser ajenas al trabajo.

Si nos vamos a un ordenador, en un momento en el que el mismo puede aglutinar el complejo completo de la empresa, en una traslación del mundo físico a un ordenador y al *software* y la nube que permite acceder, podríamos encontrar que un trabajador utiliza para su trabajo una herramienta como *Salesforce* (que en el símil presentado se podría equiparar a la máquina de empaquetado), una carpeta personal para incluir por ejemplo su reconocimiento médico o información sindical (que podría equipararse a la taquilla) y un correo corporativo y una

aplicación de *Teams* con las que se comunica con su responsable y otros compañeros sobre cuestiones laborales. Pero, en estas últimas herramientas, también puede tener lugar esa conversación de pasillo con un compañero, que no puede ser grabada por una cámara de videovigilancia con sonido. ¿Habría entonces de ser captada por un programa espía o accedida por la empresa desde el servidor del correo o mediante un registro del equipo?

Mi posición es clara, y es que no. Una de las cuestiones que aprendí en la Universidad es que, en Derecho, los principios generales son mucho más relevantes de la regulación concreta que pueda existir en cualquier rama sectorial. También, que la sociedad y los avances tecnológicos van mucho más rápido que la agenda política y legislativa de un país poniendo en jaque los preceptos de cada ley. Es ahí, justo en ese momento, a medio camino entre un escenario regulado no estrictamente aplicable y la necesaria llegada de un marco normativo que alcance la nueva realidad cuando hay que echar mano de los principios generales del Derecho.

Referencias bibliográficas

Bibliografía básica

AGUSTINA SANLLEHÍ, J. R. «Estrategias y límites en la prevención del delito dentro de la empresa: a propósito del control del correo electrónico del trabajador como posible violación de la intimidad (ex artículo 197 CP)». *InDret: Revista para el Análisis del Derecho* [en línea]. 2009, núm. 2pp. 1-43 [Consulta: 7/04/2024]. Disponible en: https://indret.com/wp-content/themes/indret/pdf/626.pdf

ALVA CRUZ, J.E. «La Intervención del Correo Electrónico Laboral por Parte Del Empleador. Entrevista al Dr. Juan Carlos Calderón Ríos». *Derecho & Sociedad* [en línea]. 2016, núm. 46, pp. 461-466. [Consulta: 7/04/2024]. ISSN 2079-3634. Disponible en:

https://dialnet.unirioja.es/servlet/articulo?codigo=7793030

BAZ RODRÍGUEZ, J. «Sentencia Del Tribunal Constitucional 170/2013, de 7 de octubre [BOE N.º 267, de 7-XI-2013]: control empresarial de la utilización, por parte de los trabajadores, de los medios informáticos de la empresa (correo electrónico). Inexistencia de vulneración de los derechos a la intimidad personal y familiar (artículo 18.1 CE)». *Ars Iuris Salmanticensis: AIS : Revista Europea E Iberoamericana De Pensamiento Y Análisis De Derecho, Ciencia Política Y Criminología* [en línea]. 2014, vol. 2, núm. 1, pp. 364-367. [Consulta: 7/04/2024]. ISSN 2340-5155. Disponible en: https://revistas.usal.es/cuatro/index.php/ais/article/view/12119/12478

CASAS BAAMONDE, M.E. «Registros empresariales sobre los trabajadores, videovigilancia e intimidad persona: necesidad de sospechas o conductas irregulares previas». *Revista de jurisprudencia laboral* [en línea]. 2022, núm. 3. [Consulta: 12/04/2024]. ISSN 2659-787X. Disponible en:

https://www.boe.es/biblioteca_juridica/anuarios_derecho/articulo.php?id=ANU-L-2022-00000001760

CUADROS GARRIDO, M.E. «Derechos digitales, protección de datos y control empresarial en España» pp. 689-717. En MATOS ZEGARRA, M. y VIDAL SALAZAR, M. (ed.). *IX Congreso Nacional de Derecho del Trabajo y de la Seguridad Social. El derecho del Trabajo y la Seguridad Social en época de cambios*. 1º ed. Lima. 2023. [Consulta: 10/05/2024] Disponible en: https://www.spdtss.org.pe/wp-content/uploads/2021/10/IX-Congreso-Nacional-full.pdf

DURO CARRIÓN, S. «El deber de Información en el articulo 87 Y 89 LOPDGDD: La quiebra de la expectativa de privacidad vinculada al derecho a la intimidad y otros derechos fundamentales en liza en la relación laboral» [en linea]. *Revista De Derecho Laboral vLex (RDLV)*. 2021, núm. 3, pp. 70-93 [Consulta: 2/05/2024]. ISSN 2696-7286. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8633783&orden=0&info=link https://dialnet.unirioja.es/servlet/extart?codigo=8633783

FERRANDO GARCÍA, M.F. «Vigilancia y control de los trabajadores y derecho a la intimidad en el contexto de las nuevas tecnologías». *Revista de Trabajo y Seguridad Social. CEF* [en linea]. 2016, núm. 399, pp. 37-68 [Consulta: 6/05/2024]. ISSN 2792- 8322. Disponible en: https://revistas.cef.udima.es/index.php/rtss/article/view/2126/1754

GARCÍA HERNÁNDEZ, P. «E-mail Archiving. Del modelo On-premise al Cloud Computing». *Archivamos* [en linea]. 2011, núm. 82 [Consulta: 28/04/2024]. Disponible en: https://publicaciones.acal.es/archivamos/article/view/80

LÓPEZ BALAGUER, M. y RAMOS MORAGUES, F.R. «Control empresarial del uso de dispositivos digitales en el ámbito laboral desde la perspectiva del derecho a la protección de datos y a la intimidad». *Lex Social. Revista de Derechos Sociales* [en línea]. 2020, vol. 10, núm.2, pp. 506-540 [Consulta: 28/04/2024]. ISSN: 2174-6419. Disponible en: https://www.upo.es/revistas/index.php/lex_social/article/view/5075

ORTEGA LOZANO, P.; GUINDO MORALES, S. «La monitorización del correo electrónico corporativo y la grabación del centro de trabajo por cámaras (visibles y ocultas)». *Trabajo y derecho: nueva revista de actualidad y relaciones laborales* [en línea]. 2020, núm. 71, p. 4. [Consulta: 06/05/2024]. ISSN-e 2386-8112. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7654495

LUNA HUERTAS, P.; MARTÍNEZ LÓPEZ, F.J.; INFANTE MORO, A.; MARTÍNEZ LÓPEZ, L., «Los sistemas de control de la actividad laboral mediante las Nuevas Tecnologías de la Información y las Comunicaciones». *Relaciones laborales. Revista crítica de teoría y práctica.* 2003, núm. 1, pp. 1403-1436. [Consulta: 02/06/2024]. ISSN 0213-0556. Disponible en: https://www.researchgate.net/publication/239590813_Los_Sistemas_de_Control_de_la_Ac

tividad Laboral Mediante las Nuevas Tecnologias de la Informacion y las Comunicaciones

LUQUE PARRA, M. y LACOMBA PÉREZ, F.R., «Acceso a dispositivos digitales del trabajador facilitados por la empresa» pp. 355-399. En RODRÍGUEZ-PIÑERO ROYO, M. y TODOLÍ SIGNES, A. (ed). *Vigilancia y control en el Derecho del Trabajo Digital*. 1ªed. Pamplona: Thomson Reuters Aranzadi, 2020.

MONEREO PÉREZ, J.L. y ORTEGA LOZANO, P.G. «El Control Empresarial Del Correo Electrónico Del Trabajador». *Temas Laborales: Revista Andaluza De Trabajo Y Bienestar Social*. 2019, núm. 150, pp. 133-159. [Consulta: 28/04/2024]. ISSN 0213-0750. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7224371

PINO PADRÓN, M.C.d., «El impacto de las tecnologías de la información en el derecho laboral, Especial Referencia a La Intimidad Del Trabajador Y El Secreto De Sus Comunicaciones». *Cadernos De Dereito Actual*. 2018. núm. 8, pp. 153-164 [Consulta: 06/05/2024]. ISSN-e 2386-5229. Disponible en:

https://dialnet.unirioja.es/servlet/articulo?codigo=6279833&orden=0&info=link https://dialnet.unirioja.es/servlet/extart?codigo=6279833

POQUET CATALÁ, R. «La protección del derecho a la intimidad del teletrabajador». *Lex Social: Revista de los derechos sociales* [en línea]. 2018, vol. 8, núm. 1, pp. 113-135. [Consulta: 10/04/2024] ISSN 2174-6419. Disponible en:

https://www.upo.es/revistas/index.php/lex_social/article/view/2918

RODRÍGUEZ ESCANCIANO, S. «Posibilidades y límites en el control de los correos electrónicos de los empleados públicos a la luz de la normativa de protección de datos». *Revista Vasca De Gestión De Personas Y Organizaciones Públicas* [en línea]. 2019. núm. 16, pp. 110-127. [Consulta: 9/06/2024] ISSN 2173-6405. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6945319&orden=0&info=link https://dialnet.unirioja.es/servlet/extart?codigo=6945319

ROLDÁN MARTÍNEZ, A.F. «Registro de las comunicaciones electrónicas del trabajador: ¿es necesaria la autorización judicial?». *Anuario de la Facultad De Derecho*. 2017, núm. 10. pp. 173-202. [Consulta: 24/04/2024] ISSN 1888-3214. Disponible

en: https://dialnet.unirioja.es/servlet/articulo?codigo=6346328&orden=0&info=link https://dialnet.unirioja.es/servlet/extart?codigo=6346328

SOUTO PRIETO, J. y BOTANA LÓPEZ, J.M. *Utilización en la empresa de las nuevas tecnologías (control empresarial e intimidad del trabajador: discurso leído el día 27 de junio de 2014 en la solemne sesión de ingreso del académico de número, Jesús Souto Prieto y contestación de José María Botana López, académico de número* [en línea]. Real Academia Gallega de Jurisprudencia y Legislación. 2014. [Consulta: 2/02/2024]Disponible en:

https://ragjyl.gal/wp-content/uploads/2016/12/Libro-Jesus-Souto-Prieto.pdf

TRUJILLO PONS, F. «El uso del correo electrónico en el ambiente laboral y el modo en que éste puede afectar al derecho a la intimidad personal y al secreto de las comunicaciones». *Revista Aranzadi de Derecho y Nuevas Tecnologías.* 2016, núm. 41, pp. 119-132. [Consulta: 9/06/2024] ISSN 1696-0351. Disponible en: https://repositori.uji.es/xmlui/bitstream/handle/10234/164466/Trujillo_2016_Uso.pdf?sequence=1&isAllowed=y

Bibliografía complementaria

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Documento de trabajo de 29 de mayo de 2002, relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo*. Disponible en: https://www.aepd.es/documento/wp249es.pdf [Consulta: 20/05/2024].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Informe 0247/2008*. Disponible en: https://www.aepd.es/documento/2008-0247.pdf [Consulta: 20/05/2024].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Informe 0615/2009*. Disponible en: https://www.aepd.es/documento/2009-0615.pdf [Consulta: 22/05/2024].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Informe 0437/2010.* Disponible en: https://www.aepd.es/documento/2010-0437.pdf [Consulta: 19/05/2024].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a la protección de datos (art. 35.4).* Mayo de 2019.

Disponible en: https://www.aepd.es/documento/listas-dpia-es-35-4.pdf [Consulta: 02/06/2023].

COMISIÓN EUROPEA. *Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto a 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* (Reglamento sobre la privacidad y las comunicaciones electrónicas), adoptada en Bruselas el 10 de enero de 2017. Disponible en: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications [Consulta: 25/05/2024].

CONSEJO DE EUROPA, TRIBUNAL EUROPEO DE DERECHOS HUMANOS (TEDH), *Manual de legislación europea en materia de la protección de datos*. 2014. Disponible en: https://rm.coe.int/09000016806ae663 [Consulta: 11/06/2024].

CONSEJO DE EUROPA, COMITÉ DE MINISTROS, *Recomendación CM/Rec (2015)5 del Comité de Ministros a los Estados miembros sobre el tratamiento de datos personales en el contexto del empleo*. Adoptada el 1 de abril de 2015. Disponible en: https://search.coe.int/cm#{%22CoEObjectId%22:[%2209000016805c3f7a%22],%22sort%22:[%22CoEValidationDate%20Descending%22]} [Consulta: 13/06/2024].

CORTES GENERALES, SENADO, *Índice en enmiendas al Proyecto de Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales* (621/000012) publicado en el Boletín Oficial de las Cortes Generales, Senado, núm. 2999,pág. 3,de 15 de diciembre de 2018. Disponible en: https://www.senado.es/legis12/publicaciones/pdf/senado/bocg/BOCG_D_12_299_2313.PDF [Consulta: 04/06/2024].

GRUPO DE TRABAJO DEL ARTÍCULO 29. *Documento de trabajo relativo a las comunicaciones electrónicas en el lugar de trabajo*, 2021. Disponible en: https://ec.europa.eu/newsroom/article29/items [Consulta: 02/06/2024].

GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, adoptado el 8 de junio de 2017, disponible en: https://www.aepd.es/documento/wp249es.pdf [Consulta: 02/06/2024].

GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 01/2017 sobre la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas, WP 247, de 4 de abril de 2017,

disponible en: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103 [Consulta: 03/06/2024].

ORGANIZACIÓN INTERNACIONAL DEL TRABAJO. *Repertorio de recomendaciones prácticas de la OIT para la protección de los datos personales de los trabajadores*, adoptada por la Oficina Internacional del Trabajo en Ginebra, 1997. Disponible en: https://www.ilo.org/es/media/270576/download [Consulta: 10/06/2024].

Legislación citada

ESPAÑA. Constitución Española. *Boletín Oficial del Estado*, de 29 de diciembre de 1978, núm. 311. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

ESPAÑA. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, de 2 de julio de 1985, núm. 157. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1985-12666

ESPAÑA. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. *Boletín Oficial del Estado,* de 19 de enero de 2018. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2008-979

ESPAÑA. Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. *Boletín Oficial del Estado*, de 24 de noviembre de 2015, núm. 255. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2015-11430

ESPAÑA. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. *Boletín Oficial de Estado*, de 6 de diciembre de 2018, núm. 294. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

ESPAÑA. Ley 10/2021, de 9 de julio, de trabajo a distancia. *Boletín Oficial del Estado*, de 10 de julio de 2021, núm. 164. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2021-11472

UNIÓN EUROPEA. 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 datos. *Diario Oficial de la Unión Europea*, de 23 de

noviembre de 1995, número 281. Disponible en: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A31995L0046

UNIÓN EUROPEA. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección civil 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). *Diario Oficial de la Unión Europea*, de 4 de mayo de 2016, núm. 119. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Jurisprudencia referenciada

Sentencia del Tribunal Europeo de Derechos Humanos (Sección Cuarta), asunto Barbulescu I contra Rumanía, núm. 61496/08, de 12 de enero de 2016, ECLI:CE:ECHR:2016:0112JUD00614968

Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala), asunto Barbulescu II contra Rumanía, núm. 61496/08, de 5 de septiembre de 2017, ECLI:CE:ECHR:2017:0905JUD006149608

Sentencia del Tribunal Europeo de Derechos Humanos (Sección Quinta), asunto Libert contra Francia, núm. 588/13, de 22 de febrero de 2018, ECLI:CE:ECHR:2018:0222JUD0058813

Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala), asunto López Ribalda II y otros contra España, núm. 1874/13 y 8567/13, de 17 de octubre de 2018, ECLI:CE:ECHR:2019:1017JUD000187413

Sentencia del Tribunal Europeo de Derechos Humanos (Sección Cuarta), asunto Copland, contra Reino Unido, núm. 62617/00, de 3 de abril de 2007, ECLI:CE:ECHR:2007:0403JUD006261700

Sentencia del Tribunal Constitucional (Sala Primera), núm. 186/2000, de 10 de julio, Recurso de amparo 2662/1997, ECLI:ES:TC:2000:186

Sentencia del Tribunal Supremo (Sala Cuarta, de lo Social, Sección 1), núm. 6128/2007, de 26 de septiembre, Recurso núm 966/2007, ECLI:ES:TSJ:2007:6128

Sentencia del Tribunal Supremo (Sala Cuarta, de lo Social, Sección 1), núm. 1323/2011, de 8 de marzo, Recurso núm 1826/2011, ECLI:ES:TSJ:2011:1323

Sentencia del Tribunal Constitucional (Sala Primera), núm. 241/2012, de 17 de diciembre, Recurso de amparo 7304/2007, ECLI:ES:TC:2012:241

Sentencia del Tribunal Constitucional (Sala Primera), núm. 29/2013, de 11 de febrero, Recurso de amparo 10522/2009, ECLI:ES:TC:2013:29

Sentencia del Tribunal Constitucional (Sala Primera), núm. 170/2013, de 17 de octubre, Recurso de amparo 2907/2011, ECLI:ES:TC:2013:170

Sentencia del Tribunal Supremo (Sala Cuarta, de lo Social, Sección 1), núm. 2618/2014, de 13 de mayo, Recurso núm 1685/2013, ECLI:ES:TS:2014:2618

Sentencia del Tribunal Supremo (Sala Cuarta, de lo Social, Sección 1), núm. 528/2014, de 16 de junio, Recurso núm 528/2013, ECLI:ES:TS:2014:2844

Sentencia del Tribunal Supremo (Sala Cuarta, de lo Social, Sección 1), núm. 119/2018, de 8 de febrero, Recurso núm 1121/2015, ECLI:ES:TS:2018:594

Sentencia del Tribunal Supremo (Sala Cuarta, de lo Social, Sección 1), núm. 489/2018, de 23 de octubre, Recurso núm 1674/2017, ECLI:ES:TS:2018:3753

Sentencia de la Audiencia Nacional (Sala de lo Social, Sección 1), núm. 3645/2022, de 22 de julio, Recurso núm 178/2022, ECLI:ES:AN:2022:3645

Sentencia del Tribunal Superior de Justicia de Andalucía (Sala de lo Social, Sección 1), núm. 7128/2003, de 9 de mayo, Recurso núm 591/2003, ECLI:ES:TSJAND:2003:7128

Sentencia del Tribunal Superior de Justicia de Madrid (Sala de lo Social, Sección 1), núm. 699/2023, de 4 de diciembre, Recurso núm 542/2003, ECLI:ES:TSJM:2023:13457

Sentencia del Tribunal Superior de Justicia de Andalucía (Sala de lo Social, Sección 1), núm. 623/2017, de 12 de julio, Recurso núm 623/2017, ECLI:ES:TSJAND:2017:10105

Sentencia del Tribunal Superior de Justicia de Canarias (Sala de lo Social, Sección 1), núm. 345/2020, de 15 de mayo, Recurso núm 22/2020, ECLI:ES:TSJICAN:2020:593

Sentencia del Tribunal Superior de Justicia de Valladolid (Sala de lo Social, Sección 1), núm. 99/2023, de 3 de marzo, Recurso núm 488/2022, ECLI:ES:JSO:2023:1191

Sentencia del Tribunal Superior de Justicia de Cataluña (Sala de lo Social, Sección 1), núm. 2418/2022, de 20 de abril, Recurso núm 7603/2022, ECLI:ES:TSJCAT:2022:3612

Sentencia del Tribunal Superior de Justicia de Canarias (Sala de lo Social, Sección 1), núm. 347/2023, de 21 de abril, Recurso núm 964/2022, ECLI:ES:TSJICAN:2023:825

Sentencia del Tribunal Superior de Justicia de Aragón (Sala de lo Social, Sección 1), núm. 454/2022, de 13 de junio, Recurso núm 413/2022, ECLI:ES:TSJGAL:2022:1050

Sentencia del Tribunal Superior de Justicia de Galicia (Sala de lo Social, Sección 1), núm. 5126/2022, de 11 de noviembre, Recurso núm 4825/2022, ECLI:ES:TSJGAL:2022:7629

Sentencia del Tribunal Superior de Justicia de Canarias (Sala de lo Social, Sección 1), núm. 87/2024, de 8 de febrero, Recurso núm 585/2023, ECLI:ES:TSJICAN:2024:270

Sentencia del Tribunal Superior de Justicia de Madrid (Sala de lo Social, Sección 1), núm. 405/2023, de 8 de junio, Recurso núm 207/2023, ECLI:ES:TSJM:2023:6861

Sentencia del Juzgado de lo Social de Badajoz nº 2, núm. 104/2019, de 9 de abril, Recurso núm 91/2019, ECLI:ES:JSO:2019:1339

Sentencia del Juzgado de lo Social de Vigo nº 5, núm. 564/2022, de 30 de diciembre, Recurso núm 842/2021, ECLI:ES:JSO:2022:7918

Web

ActiveTrack. 8 de junio, 11:00. Disponible en: https://www.activtrak.com/

Clever control Smart Employee Monitoring. 8 de junio, 9:32. Disponible en: https://clevercontrol.com/es/best-employee-monitoring-software/

Slack. 7 de junio, 21:46. Disponible en: https://slack.com/intl/es-es/

Spyrix Employee Monitoring. 8 de junio. 10: 42. Disponible en:

https://www.spyrix.com/es/employee-monitoring.php

Teams. 7 de junio, 20:03. Disponible en: https://www.microsoft.com/es-es/microsoft-teams/group-chat-software

Linka Ciberseguridad Gestionada. 13 de junio, 19:22. Disponible en: https://www.grupolinka.com/control-ordenadores-empleados/

Listado de abreviaturas

AEPD	Agencia Española de Protección de Datos
Art.	Artículo
Arts.	Artículos
CE	Constitución Española
CEDH	Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales
DLP	*Data Loss Prevention* (Prevención de pérdida de datos)
ET	Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el Texto Refundido de la Ley del Estatuto de los Trabajadores
EIPD	Evaluación de Impacto relativa a la Protección de Datos
GT29	Grupo de Trabajo del Artículo 29
IT	Tecnologías de la Información
LOPDGDD	Ley Orgánica 3/2028, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales
NGFW	*Next Generation Firewall* (Firewall de nueva generación)
LOPJ	Ley Orgánica del Poder Judicial
OIT	Organización Internacional del Trabajo
RD	Real Decreto
RGPD	Reglamento General de Protección de Datos: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección civil de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos y por el que se deroga la Directiva 95/46/CE
STS	Sentencia del Tribunal Supremo
TEDH	Tribunal Europeo de Derechos Humanos
UTM	*Unified Threat Management* (Gestión unificada de amenazas)

Anexo A. TEAMS

Informe	Público	GCC	GCCH	Dod	¿Qué se mide?
Informes de uso de Teams	Sí	Sí	Sí	Sí	Usuarios activos Usuarios activos en equipos y canales Canales activos Mensajes Configuración de privacidad de teams Invitados activos en un equipo Usuarios externos activos (en canales compartidos) Detalles específicos del canal compartido en un equipo (nuevo)
Informe de actividad de usuario de Teams	Sí	Sí	Sí	Sí	Usuarios activos internos y externos (en canales compartidos) Mensajes que un usuario publicó en un chat de equipo Mensajes que un usuario publicó en un chat privado 1:1 llama a un usuario en el que ha participado Número de reuniones organizadas por el usuario Número de reuniones en las que el usuario ha participado Audio, vídeo y tiempo de uso compartido de pantalla de reuniones Fecha de la última actividad de un usuario Interacciones de canal compartidas de un usuario (nuevo)
Informe de uso de dispositivos de Teams	Sí	Sí	Sí	Sí	Usuarios de Windows Usuarios de Mac Usuarios de iOS Usuarios de teléfonos Android
Informe de uso de aplicaciones de Teams (nuevo)	Sí	Sí	No	No	Total de usuarios activos de la aplicación Total de equipos activos que usan la aplicación Total de aplicaciones instaladas (nuevas) Total de aplicaciones inactivas Uso total de aplicaciones de 1P frente a 3P frente a lob (nuevo)

Informe	Público	GCC	GCCH	Dod	¿Qué se mide?
Informe de uso de eventos en directo de Teams	Sí	Sí	No	No	Vistas totales Hora de inicio Estado del evento Organizador Presentador Productor Configuración de la grabación Tipo de producción
Informe de usuarios bloqueados de RTC de Teams	Sí	Sí	No	No	Nombre para mostrar Número de teléfono Motivo Tipo de acción Fecha y hora de la acción
Informe de grupos de minutos de RTC de Teams	Sí	Sí	No	No	País o región Funcionalidad (licencia) Minutos totales Minutos usados Minutos disponibles
Informe de uso de RTC de Teams: Planes de llamadas	Sí	Sí	No	No	Marca de tiempo Nombre de usuario Número de teléfono Tipo de llamada Llamado a País o región Se ha llamado desde Desde el país o la región Cargo Moneda Duración Nacional e internacional Id. de llamada Tipo de número País o región Id. de conferencia Funcionalidad (licencia)

Informe	Público	GCC	GCCH	Dod	¿Qué se mide?
Informe de uso de RTC de Teams: enrutamiento directo	Sí	Sí	Sí	Sí	Marca de tiempo Nombre para mostrar Dirección SIP Número de teléfono Tipo de llamada Llamado a Hora de inicio Hora de invitación Tiempo de error Hora de finalización Duración Tipo de número Omisión de medios SBC FQDN Región de Azure Tipo de evento Código SIP final Subcódigo final de Microsoft Frase SIP final Id. de correlación
Informe de licencia de protección de la información de Teams	Sí	Sí	No	No	Si los usuarios tienen licencias válidas para enviar sus mensajes a través de notificaciones de cambio Número total de eventos de notificación de cambios desencadenados por un usuario Qué aplicaciones escuchan los eventos de notificación de cambios de toda la organización
Informe de uso de Teams Citas virtuales	Sí	Sí	No	No	Número de citas virtuales Número de citas Bookings Número de citas integradas con registros electrónicos de salud (EHR) de Teams Duración media de una cita Promedio de tiempo de espera en la sala de espera de los asistentes Hora de inicio Id. de reunión

Informe	Público	GCC	GCCH	Dod	¿Qué se mide?
					Tiempo de espera en la sala de espera Duración Estado Tipo de producto Asistentes Departamento SMS enviados Si la cita usó una funcionalidad avanzada de Citas virtuales
Informe de actividad de Citas virtuales avanzado de Teams	Sí	Sí	No	No	Número de usuarios que usan funcionalidades avanzadas de Citas virtuales Número de usuarios que usan notificaciones de texto SMS Número de usuarios que realizan citas a petición Número de usuarios que usan la cola
Informe de Citas virtuales del conector EHR de Teams	Sí	Sí	No	No	Hora de inicio Duración Principal (nombre del organizador de la reunión) Correo electrónico del principal (correo electrónico del organizador de la reunión) Departamento Asistentes Tiempo de espera en la sala de espera Si la cita está dentro del límite de asignación
Informe de uso y rendimiento de Walkie Talkie	Sí	Sí	No	No	Las métricas incluyen el número de transmisiones push-to-talk (PTT) realizadas y recibidas, la actividad del canal, la duración de la transmisión y los detalles del dispositivo y los participantes.
Informe de uso de notificaciones SMS	Sí	No	No	No	Tiempo de envío Enviado desde Tipo de notificación sms Tipo de producto Estado
Nuevo informe de uso de Teams	Sí	Sí	No	No	Información general sobre los equipos de escritorio cliente de Teams en su organización

Tabla obtenida de: https://learn.microsoft.com/es-es/microsoftteams/teams-analytics-and-reports/teams-reporting-reference

Anexo B. MICROSOFT CORREO ELECTRÓNICO

Elemento	Descripción
Nombre de usuario	La dirección de correo electrónico del usuario.
Nombre para mostrar	Nombre completo del usuario.
Deleted	Hace referencia al usuario cuyo estado actual se elimina, pero que estuvo activo durante alguna parte del período de informes del informe.
Fecha de eliminación	La fecha en que se eliminó el usuario.
Fecha de la última actividad	La última vez que el usuario realizó una actividad de lectura o envío de correo electrónico.
Acciones de envío	El número de veces que se registró una acción de envío de correo electrónico para el usuario.
Acciones de recepción	El número de veces que se registró una acción de recepción de correo electrónico para el usuario.
Acciones de lectura	El número de veces que se registró una acción de lectura de correo electrónico para el usuario.
Acciones creadas para reuniones	El número de veces que se registró una acción de envío de una convocatoria de reunión para el usuario.
Reuniones de acciones interactuadas	El número de veces que se registró una acción de aceptación, tentativa, declinación o cancelación de una convocatoria de reunión para el usuario.
Producto asignado	Productos asignados a este usuario.

Tabla extraída de: https://learn.microsoft.com/es-es/microsoft-365/admin/activity-reports/email-activity-ww?view=o365-worldwide

Anexo C. SLACK

Canales

Creado	La fecha de creación del canal
Espacios de trabajo*	Espacios de trabajo dentro de una organización de Enterprise Grid en los que se comparte el canal con
Organizaciones externas	Organizaciones externas en el canal de Slack Connect
Activo por última vez	La fecha en la que se envió el último mensaje en el canal
N.º total de miembros	Número de personas en el canal, incluidos los miembros plenos y los invitados
Miembros plenos	Número de miembros plenos en el canal
Invitados	Número de invitados en el canal
Mensajes publicados	Número de mensajes enviados en el canal, incluidos mensajes de aplicaciones y bots
Mensajes publicados por miembros	Número de mensajes enviados por miembros en el canal
Miembros que publicaron	Número de personas que publicaron mensajes en el canal
Miembros que han visto	Número de personas que han visto el canal
Variación en miembros diarios que publicaron	Porcentaje que refleja el número de personas que publicaron en el canal en los últimos 30 días, en comparación con los 30 días anteriores
Reacciones añadidas	Número de reacciones que se han añadido a los mensajes en el canal
Miembros que reaccionaron	Número de personas que añadieron reacciones en el canal
Juntas iniciadas*	Número de juntas que se han creado o unido en el canal, con una duración superior a cinco segundos y con, al menos, otro miembro

*Esta métrica solo está disponible en paneles de nivel de espacio de trabajo de organizaciones de Enterprise Grid.

Métricas de los miembros de Enterprise Grid a nivel de organización

Recuento de Juntas de Slack	Número total de juntas organizadas o presenciadas, con una duración superior a cinco segundos y con, al menos, otro miembro
Activo con Slack Connect	Si el miembro ha leído o publicado (o no) un mensaje a un canal o mensaje directo compartido con, al menos, un espacio de trabajo externo
Activo con aplicaciones	Si el miembro ha interactuado (o no) con una aplicación de Slack o integración personalizada, o si esa aplicación o integración ha llevado a cabo una acción en nombre del miembro en cuestión.
Activo con flujos de trabajo	Si el miembro ha interactuado (o no) con al menos un flujo de trabajo
Recuento de búsquedas	Número de búsquedas que un miembro ha realizado en Slack

Espacios de trabajo

URL	URL del espacio de trabajo
Creado	Fecha en la que se creó tu espacio de trabajo
Activo por última vez	La fecha en la que se envió el último mensaje en el espacio de trabajo
N.º total de miembros	Número de personas en el espacio de trabajo, incluidos los miembros plenos y los invitados

Miembros plenos	Número de miembros plenos en el espacio de trabajo
Invitados	Número de invitados en el espacio de trabajo
Aplicaciones	Número de aplicaciones instaladas en el espacio de trabajo
Canales abiertos, espacio de trabajo único	Número de canales abiertos del espacio de trabajo
Canales abiertos que pertenecen a varios espacios de trabajo	Número de canales abiertos que pertenecen a varios espacios de trabajo del espacio de trabajo
Miembros activos	Número de personas que han leído o enviado un mensaje en al menos un canal o mensaje directo del espacio de trabajo
Miembros activos (%)	Porcentaje que refleja el número de personas que han leído o enviar un mensaje en este espacio de trabajo en comparación con otros espacios de trabajo de la organización
Variación en miembros activos	Porcentaje que refleja el número de personas que publicaron en el canal en los últimos 30 días, en comparación con los 30 días anteriores
Miembros que publicaron	Número de personas que publicaron mensajes en el espacio de trabajo
Archivos subidos	Número de archivos subidos a canales en el espacio de trabajo
Mensajes publicados por miembros	Número de mensajes enviados por miembros en el espacio de trabajo

Mensajes en canales abiertos, espacio de trabajo único	Número de mensajes enviados en canales abiertos del espacio de trabajo
Porcentaje de mensajes, canales abiertos	Porcentaje que refleja el número de personas que publicaron en canales abiertos en comparación con canales cerrados y mensajes directos del espacio de trabajo
Porcentaje de visualizaciones, canales abiertos	Porcentaje que refleja el número de personas que visualizaron canales abiertos en comparación con canales cerrados y mensajes directos del espacio de trabajo
Mensajes en canales que pertenecen a varios espacios de trabajo	Número de mensajes enviados en canales abiertos compartidos en varios espacios de trabajo de tu organización
Mensajes en canales cerrados	Número de mensajes enviados en canales cerrados

Tabla extraída de: https://slack.com/intl/es-es/help/articles/360057638533-C%C3%B3mo-interpretar-la-informaci%C3%B3n-de-tu-panel-de-an%C3%A1lisis-de-datos