Machine Translated by Google

CNS 39/2021

Dictamen en relación con la consulta de un Ayuntamiento en relación con el acceso al equipo local de un funcionario del Ayuntamiento, a efectos de poder acceder a información del Ayuntamiento

Se presenta ante la Autoridad Catalana de Protección de Datos un escrito de un Ayuntamiento, en el que se pide Dictamen a esta Autoridad en relación con la posibilidad de acceder al equipo local que utiliza un funcionario del Ayuntamiento, que se encuentra en situación de baja, para poder acceder a información propiedad del Ayuntamiento, a través de su departamento informático.

Analizada la petición, que no se acompaña de mayor información, vista la normativa vigente aplicable y de acuerdo con el informe de la Asesoría Jurídica, se dictamina lo siguiente.

(...)

II

La consulta se refiere a la posibilidad de acceso al equipo local que utiliza un funcionario del Ayuntamiento, que se encuentra en situación de baja, a efectos de poder acceder a documentación de la Concejalía de Participación Ciudadana del Ayuntamiento. La consulta explica que el funcionario "es el único usuario que centraliza esta Concejalía, y por tanto crea y guarda la documentación." Según la consulta, no poder acceder a esta información paraliza y afecta al desarrollo de las acciones del Ayuntamiento, y añade que el funcionario en cuestión tiene un asunto disciplinario con el Ayuntamiento, todavía pendiente de resolución.

La consulta añade que los funcionarios del Ayuntamiento recibieron formación en protección de datos y se les explicó el protocolo de seguridad del Ayuntamiento (entre otros, que no se permiten temas personales en las herramientas de trabajo del Ayuntamiento, que se ha comunicado a los trabajadores la posibilidad de accesos a todas las herramientas de control titularidad del Ayuntamiento, y que se prevé que es necesario guardar toda la documentación en espacios habilitados).

En este punto, conviene recordar que, más allá de que las referencias hechas en la consulta a algunos apartados de dicho protocolo sirvan para enmarcar el supuesto planteado, el objeto de este informe no es hacer una valoración o validación de la adecuación del protocolo del Ayuntamiento en la normativa de protección de datos.

Dicho esto, la consulta plantea "si podemos acceder al equipo local en el que desarrolla sus funciones un funcionario del Ayuntamiento, a efectos de poder acceder a información propiedad del Ayuntamiento, a través del Departamento informático del Ayuntamiento, por las siguientes finalidades :

Traducción Automática

Machine Translated by Google

A) Poner toda la documentación que pueda existir de la Concejalía mencionada en los espacios destinados al efecto B) Garantizar la integridad de la documentación dado que no está en un espacio donde se realizan copias de seguridad C) Corroborar si se está incumpliendo las medidas de seguridad del Ayuntamiento, posibilidad de que esta comunicada y aceptada por los funcionarios D) Desbloquear la parálisis de la Concejalía, entendiendo que es una medida proporcionada y el bien a proteger es mayor al que se podría perjudicar. Es decir, el desarrollo de una Concejalía, -interés general y múltiples afectados- es más importante que el acceso al equipo de una funcionaria, donde podría, y recalcamos "podría", existir información personal, en la que en ningún caso, queremos acceder E) Que cualquier actuación sea escrupulosa con la posibilidad de encuentro de documento de carácter privado, aunque están prohibidos temas personales en las herramientas de trabajo, velando y evitando en este caso, cualquier apertura y acceso en estos contenidos F) Que l acceso sería hecho por el Administrador de sistemas externo – informático G) Si entienden que debe comunicarse esta acción al afectado, en caso de que consideren que se puede hacer el acceso, aunque la consulta se hace desde la perspectiva que el afectado no presta su consentimiento."

Según la consulta, ésta se plantea "desde la perspectiva de que el afectado no presta su consentimiento." Teniendo esto en cuenta, partiendo de la premisa de que en el caso planteado el Ayuntamiento no dispondría del consentimiento del trabajador, habrá que ver si concurre alguna de las bases jurídicas del artículo 6.1 RGPD, que permitan considerar lícito el tratamiento de datos, y en qué condiciones.

III

Según dispone el artículo 87 del LOPDDDD:

> **"1. Los trabajadores y empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.**
>
> **2. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.**
>
> **3. 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 derechos reconocidos constitucional y legalmente. En su elaboración tendrán que participar los representantes de los trabajadores.**
>
> **El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.**
>
> **Los trabajadores deberán ser informados de los criterios de utilización a que se refiere este apartado."**

Traducción Automática

Machine Translated by Google

También hay que tener en cuenta diversas previsiones de la normativa de ámbito laboral, en relación con la licitud de las medidas de control por parte del empresario -en este caso, una Administración pública-, del cumplimiento por parte de los trabajadores, de las sus obligaciones laborales.

Especialmente, el artículo 52 del Estatuto básico del trabajador público (EBEP), según el cual: "Los empleados públicos deberán desempeñar con diligencia las tareas que tengan asignadas y velar por los intereses generales con sujeción y observancia de la Constitución y del resto del ordenamiento jurídico (...)", y el artículo 20.3 del Estatuto de los Trabajadores (ET), según el cual: "El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad (...)".

Desde la perspectiva de la normativa de protección de datos, como se desprende del artículo 87 del LOPDGDD, las finalidades para las que resultaría lícita la monitorización de los equipos que el empresario pone a disposición de los trabajadores, serían, de por un lado, el control del cumplimiento de las obligaciones laborales del trabajador (en conexión con las previsiones de la normativa laboral), y por otro, la de garantizar la integridad de los dispositivos que utilizan los trabajadores para el desarrollo de sus funciones .

En el caso examinado, y según la información disponible, el Ayuntamiento (responsable del tratamiento ej. art. 4.7 RGPD), apunta a que la finalidad principal del acceso al equipo asignado al funcionario que se encuentra de baja sería la de asegurar la continuidad del trabajo llevado a cabo desde el Ayuntamiento puesto que, según el Ayuntamiento, la documentación guardada en el equipo local que utiliza el trabajador sería "esencial para poder seguir con la actividad que desarrolla la Concejalía ").

Hacemos notar que los "fines" a los que se refieren las preguntas A) y D) de la consulta ("Poner toda la documentación que pueda existir de la Concejalía en los espacios destinados al efecto" y "Desbloquear la parálisis de la Concejalía (...)"), dada la información de que se dispone, parece que se refieren o relacionan con esta finalidad general de aseguramiento del cumplimiento de las funciones que se llevan a cabo desde la Concejalía del Ayuntamiento.

A esto hay que añadir que la pregunta B) "Garantizar la integridad de la documentación dado que no está en un espacio donde se realizan copias de seguridad", según la información de que se dispone, también se referiría a la finalidad de acceder al equipo en cuestión para proteger la documentación de la Concejalía y por tanto, para asegurar el trabajo desarrollado desde el Ayuntamiento.

Como ha admitido la jurisprudencia (a modo de ejemplo, la STC 61/2021, a la que nos remitimos), el empresario puede establecer controles sobre el uso de las herramientas que pone a disposición de los trabajadores. Especialmente relevante es la STEDH, caso Barbulescu, de 5 de septiembre de 2017, en la que el TEHDH establece determinados elementos que debería aplicarse en este contexto. En síntesis, el TEDH hace referencia a la información que debe darse a los trabajadores respecto a las medidas que puede tomar el empresario para supervisar estas herramientas, en particular, las comunicaciones de los trabajadores; cuál es el alcance de la supervisión, o si el empresario ha valorado la existencia de medidas de control menos intrusivas para los trabajadores, entre otros (apartado 210 de la STEDH de 5 de septiembre de 2017, a lo que nos remitimos).

Según la consulta, el protocolo del Ayuntamiento hace referencia a que el responsable del tratamiento "informa igualmente a los usuarios que se procederán a eventuales controles

Traducción Automática

Machine Translated by Google

(contenido del PC, correo electrónico, conexiones internet, servidores y softwares contratados) (...).”

Recuerda que esta Autoridad ha dictado la Recomendación 1/2013, sobre el uso del correo electrónico en el ámbito laboral (disponible en la web www.apdcat.cat), en la que se hacen diferentes consideraciones que resultan de especial interés en este caso, ya la que nos remitimo

En el apartado III de la Recomendación, referido al acceso al correo electrónico por parte de la empresa, se recuerda también que el medio y el alcance del control debe ser proporcionado a la finalidad que se persiga, y es identifican los objetivos que podrían justificar el acceso, en este caso, a los equipos u otros dispositivos que el empresario pone a disposición de los trabajadores, con el fin de acceder a la documentación de la Concejalía.

En concreto, la Recomendación identifica la posibilidad de acceso con el fin de garantizar la continuidad de la actividad en ausencia de la persona trabajadora (vacaciones, enfermedad, etc.), teniendo en cuenta que la ausencia de un trabajador, especialmente si es de larga duración, puede acarrear problemas para la continuidad normal de la actividad, si no se puede acceder a determinada información que, en el caso que nos ocupa, se encontraría en el equipo de que dispone el trabajador en situación de baja. Especialmente teniendo en cuenta que, según la consulta, este trabajador es "el único usuario que centraliza la información de la Concejalía", lo que habría provocado, siempre según la consulta, la parálisis de las funciones llevadas a cabo por ésta.

También añadimos que, según se pone de manifiesto en el apartado III de la Recomendación -y dado que se desconoce si el protocolo del Ayuntamiento lo ha previsto-, es recomendable que, cuando la intervención viene justificada para esta finalidad de asegurar la continuidad de la actividad laboral, "es conveniente, si es posible, planificar las medidas que se adoptarán para garantizar la continuidad durante la ausencia" y, si esto no es posible, haría falta que el órgano superior del trabajador "valore de forma motivada la necesidad de la intervención para la continuidad del servicio.”

En aplicación del principio de responsabilidad proactiva (art. 5.2 RGPD), el responsable, en este caso, el Ayuntamiento, debe responder del cumplimiento de los principios de protección de datos, y por eso, a los efectos que interesan, no sería suficiente en el ·legar una finalidad para el acceso que en términos generales puede ser lícita, sino que deberá motivarse en base a las circunstancias de cada caso.

En este caso, la consulta expone que la documentación depositada en el equipo local del trabajador que se encuentra en situación de baja, es esencial para poder seguir con la actividad que desarrolla la Concejalía, y que no poder acceder a la información de la Concejalía paraliza y afecta al desarrollo de las acciones que se realizan en el Ayuntamiento, de modo que, siempre según la consulta, desde la baja del trabajador no se ha podido continuar con la actividad normal de la Concejalía.

Hacer notar, en cualquier caso que con carácter general haría falta que el Ayuntamiento valore los riesgos que para la información del Ayuntamiento debe tratar se almacene de manera local en equipos de los que no existe una copia de seguridad. La garantía de la integridad y la disponibilidad de la información requeriría almacenar la información mediante sistemas que permitan realizar de forma periódica copias de seguridad periódicas, que debería custodiar el Ayuntamiento.

Teniendo en cuenta todo lo expuesto, y dada la información de que se dispone, en principio se podría considerar que el tratamiento objeto de consulta podría ser lícito para el cumplimiento de esta finalidad (garantizar la continuidad del trabajo de la Concejalía en ausencia del trabajador que se encuentra en situación de baja), a efectos de la previsión del artículo 6.1

Traducción Automática

Machine Translated by Google

apartado e) del RGPD, en conexión con las previsiones normativas a las que hemos mencionado (normativa laboral y art. 87 LOPDGDD). Esto, siempre que resulte necesario para asegurar el normal funcionamiento del trabajo desarrollado desde la Concejalía del Ayuntamiento -como parece que sería el caso examinado, dada la información disponible-.

IV

Aún en relación con la licitud del acceso, la pregunta C), pregunta si se podría justificar el acceso al equipo del trabajador, por "Corroborar si se está incumpliendo las medidas de seguridad del Ayuntamiento, posibilidad que está comunicada y aceptada por los funcionarios".

Parece, por la información disponible, que en este caso el Ayuntamiento plantea si el acceso no ya sobre la base de una finalidad de garantizar la continuidad de la actividad de la Concejalía -cuestión ya comentada-, sino para comprobar el incumplimiento -por parte del trabajador- de las medidas de seguridad que, por la información de que se dispone, el Ayuntamiento podría haber previsto en el protocolo correspondiente.

Cabe recordar que, según explica la consulta, en el caso planteado el funcionario en cuestión "tiene un asunto disciplinario con el Ayuntamiento, todavía pendiente de resolución."

Por la información disponible, se desconoce si el asunto disciplinario referido por el Ayuntamiento tiene vinculación alguna con un posible mal uso del trabajador de los medios (equipo informático, correo electrónico, etc), que el Ayuntamiento habría puesto a su disposición, o si el acceso al equipo, objeto de consulta, puede ser relevante o necesario a estos efectos, y en medida.

A la vista de la información disponible, este informe no puede determinar si los posibles indicios de mal uso o de "posible incumplimiento de las medidas de seguridad" por parte del trabajador, de que pueda disponer el Ayuntamiento, serían suficientes a efectos de justificar o considerar lícita o proporcionada la intervención del equipo del trabajador en el caso concreto que se analice.

Hecha esta consideración, y en términos generales, conviene recordar que, según el artículo 87.2 LOPDGDD, se considera lícito el acceso del empresario a contenidos derivados del uso de los medios que facilita a sus trabajadores, para "garantizar la integridad de estos dispositivos".

En la medida, que la finalidad pretendida por el Ayuntamiento, tenga por objetivo detectar posibles incumplimientos de las medidas de seguridad que éste haya previamente puesto en conocimiento de los trabajadores a través del protocolo o de la formación que se habría dado a los trabajadores y, en definitiva, garantizar el uso adecuado del equipo puesto a disposición del trabajador y la integridad y seguridad de la información y documentación contenida en el mismo, en principio podría entenderse que el acceso responde a una finalidad prevista en la misma normativa que, por tanto, puede ser lícita.

En este sentido, como recuerda esta Autoridad en la Recomendación 1/2013, el acceso fundamentado en la finalidad de constatar un posible mal uso de los equipos que el Ayuntamiento pone a disposición de los trabajadores), debe ser proporcionado al tipo de riesgo que pueda derivarse del mal uso del equipo o de la cuenta de correo del trabajador, en los términos que se apuntan en el punto 3 del apartado III de la Recomendación.

Por tanto, para considerar lícito el acceso al equipo del trabajador para corroborar el correcto cumplimiento de las "medidas de seguridad" a que se refiere la consulta, habría que previamente identificar este riesgo, y determinar si no existen medidas alternativas menos

Traducción Automática

Machine Translated by Google

intrusivas para realizar esta comprobación, tal y como se desprende de la normativa y de la jurisprudencia mencionadas.

V

En cuanto a la pregunta E): "Que cualquier actuación sea escrupulosa con la posibilidad de encuentro de documento de carácter privado, aunque están prohibidos temas personales en las herramientas de trabajo, velando y evitando en este caso, cualquier apertura y acceso en estos contenidos", es necesario realizar las siguientes consideraciones.

La consulta hace referencia a que los funcionarios del Ayuntamiento recibieron formación en protección de datos y que el protocolo de seguridad del Ayuntamiento prevé, entre otros, que "los recursos de la entidad no pueden utilizarse para fines privados".

A efectos de la normativa de protección de datos, hay que tener en cuenta -como se desprende del apartado III de la Recomendación 1/2013-, que aunque el Ayuntamiento haya determinado que los trabajadores no pueden hacer uso de los equipos, o del correo electrónico por motivos personales o ajenos al ámbito laboral (en caso de que nos ocupa, el protocolo del Ayuntamiento determinaría que "los recursos de la entidad no pueden utilizarse con fines privados"), el trabajador no siempre podrá evitar , por ejemplo, el uso que hagan terceras personas de estos correos, para remitirle mensajes de carácter personal.

De la misma forma, si bien el protocolo del Ayuntamiento, por la información disponible, indica la prohibición de tener documentación personal en los equipos que la empresa facilita a los trabajadores, no es descartable que el acceso al equipo del trabajador , que puede ser lícito en los términos apuntados, comporte el acceso a información personal del propio trabajador

Desde la perspectiva de los principios de protección de datos, se valora positivamente la previsión que explicita la consulta, en el sentido de que la actuación del Ayuntamiento deberá ser escrupulosa en caso de que se encuentre documentación de tipo privado, "evitando en éste caso de cualquier apertura y acceso" de estos contenidos.

Al respecto, recordar que el principio de minimización (art. 5.1.c) RGPD) exige que los datos tratados deben ser los adecuados, pertinentes y limitados a lo necesario en relación con las finalidades del tratamiento. En caso de que nos ocupe, dadas las finalidades mencionadas (previstas en el artículo 87 LOPDGDD, en conexión con la normativa laboral estudiada), que pueden habilitar el acceso y monitorización de los equipos que la empresa pone a disposición de los trabajadores, no parece proporcionado ni justificado, en principio, el acceso a información privada en los términos de la consulta.

Por tanto, tal y como apunta la misma consulta, y en línea con lo que recuerda esta Autoridad en la Recomendación 1/2013, vistas las finalidades del acceso al equipo del trabajador según se desprende de la información aportada, sería necesario articular la intervención en el equipo del trabajador, evitando el acceso a este contenido de tipo privado o ajeno a la documentación de la Concejalía.

En este sentido respondiendo a la pregunta F resulta conveniente limitar el acceso a las personas que sea estrictamente necesario para el ejercicio de sus funciones, realizar la intervención a partir de una copia o duplicado de la información almacenada, sin alterar la información que conste en el equipo, y documentar tanto la intervención como las actuaciones posteriores describiendo de forma detallada las actuaciones realizadas y los resultados obtenidos.

Traducción Automática

Machine Translated by Google

Según la Recomendación 1/2013, en este caso el acceso debería llevarlo a cabo la persona designada por el responsable de seguridad, en presencia de la persona trabajadora o, si no es posible, del representante del personal y de la persona instructora o inspectora.

En relación con esta cuestión, en la consulta se indica "Que el acceso sería hecho por el Administrador de sistemas externo -informático-".

Aunque se prevea la intervención de un técnico externo, el acceso al equipo del trabajador, y el tratamiento de la información a la que se acceda, deberá producirse siguiendo las indicaciones del Ayuntamiento. En este caso en que el acceso se lleva a cabo por un tercero externo y ajeno al responsable, correspondería al Ayuntamiento establecer cómo se debe producir este acceso al equipo y el consiguiente tratamiento de la información, a través de un contrato o acuerdo de encargo del tratamiento, en los términos previstos en el artículo 28 RGPD, al que nos remitimos.

Esto, sin perjuicio de que, tanto si el acceso se lleva a cabo desde servicios propios del Ayuntamiento, como si se articula a través de un contrato de encargo para que acceda un tercero ajeno al Ayuntamiento (como una empresa externa), cualquier tratamiento de datos personales se encuentra sujeto al necesario cumplimiento del principio de confidencialidad (art. 5.1.f) RGPD), que obliga a cualquier persona que acceda a los datos personales que puedan contenerse en la documentación, archivos, o correo electrónico, en su caso, del equipo del trabajador en cuestión.

Es responsabilidad del Ayuntamiento, en cualquier caso, informar a cualquiera de las personas designadas para intervenir en el acceso al equipo del trabajador, de sus deberes y obligaciones en materia de seguridad, y en especial de este deber de secreto .

En este sentido, como recuerda la Recomendación 1/2013, en este sentido puede ser recomendable hacer firmar a las personas que intervienen en estas operaciones, un compromiso de confidencialidad respecto de los datos a los que puedan tener acceso.

VI

En cuanto a la pregunta G): "Si entienden que debe comunicarse esta acción al afectado, en caso de que consideren que se puede hacer el acceso, aunque la consulta se hace desde la perspectiva que el afectado no presta su consentimiento.", hay que decir lo siguiente:

Cómo se desprende del artículo 87.3 in fine LOPDGDD, y cómo se pone de manifiesto no sólo en la RGPD y la jurisprudencia mencionada (STEDH Barbulescu y STC 61/2021, entre otros), sino también en la Recomendación 1/ 2013, teniendo en cuenta que la monitorización de los equipos que el empresario pone a disposición de los trabajadores puede ser considerada una medida intrusiva, es necesario asegurar que los trabajadores, en este caso, el trabajador que se encuentra de baja, tienen conocimiento de ello.

Como recuerda la Recomendación 1/2013 (apartado III), el acceso a las cuentas de correo del trabajador y, por extensión, podríamos añadir, a los equipos que éste emplea por razones de trabajo, debe llevarse a cabo de acuerdo con las normas de uso que aprueba la empresa, "que deben advertir sobre los mecanismos de control del uso de las tecnologías que puedan afectar a la privacidad de las personas, de las consecuencias que se pueden derivar del control y las garantías para las personas trabajadoras, en especial el derecho a ser informado."

Dicho esto, respecto en qué momento se debería informar al trabajador dada la finalidad que se persigue, recordemos que, según se expone en el apartado III de la Recomendación 1/2013, en el caso del acceso a garantizar la continuidad de la actividad del Ayuntamiento en ausencia,

Traducción Automática

Machine Translated by Google

en este caso por enfermedad, del trabajador, debería comunicarse previamente a éste, y con suficiente antelación a la intervención. Sólo si no fuera posible esta comunicación previa, se podría informar al trabajador con posterioridad, a la mayor brevedad posible.

En cuanto al acceso con el fin de detectar un posible mal uso del equipo por parte del trabajador, se considera que igualmente la intervención debería ponerse en conocimiento previo del trabajador afectado, salvo que el Ayuntamiento considere que esto puede obstaculizar las investigaciones adecuadas.

Por último, recordar que, por aplicación de las obligaciones del responsable en materia de protección de datos (arts. 12, 13 y 14 RGPD), el Ayuntamiento debe facilitar información a los trabajadores en relación con la posibilidad de ejercer sus derechos de acceso, rectificación o supresión de sus datos, entre otros (arts. 15 y ss. RGPD). Esto, independientemente de cuál sea la base jurídica del tratamiento (art. 6.1 RGPD).

De acuerdo con las consideraciones hechas en este informe en relación con la consulta planteada, se hacen las siguientes,

Conclusiones

El acceso al equipo local del funcionario que se encuentra de baja, con el fin de garantizar la continuidad de la actividad en ausencia del trabajador y con el fin de comprobar un posible mal uso del equipo por parte del trabajador y proteger la integridad de la información, puede considerarse lícito si resulta justificado por las circunstancias concurrentes.

Es necesario articular la intervención en el equipo del trabajador, de forma que se evite el acceso a contenido de tipo privado o ajeno a la documentación de la Concejalía.

El acceso con el fin de garantizar la continuidad de la actividad en ausencia del trabajador, se le comunicará previamente a la intervención, salvo que no sea posible. El acceso con el fin de determinar un mal uso del equipo, también se pondrá en conocimiento del trabajador, salvo que obstaculice las investigaciones oportunas. Se realizará en presencia de la persona trabajadora o, si no fuera posible, del representante del personal.

El acceso debe limitarse a las personas que sea estrictamente necesario que deben quedar vinculadas por el deber de confidencialidad. El acceso debe realizarse a partir de una copia o duplicado de la información almacenada, sin alterar la información que conste en el equipo, y documentar tanto la intervención como las actuaciones posteriores describiendo de forma detallada las actuaciones realizadas y los resultados obtenidos. Si interviene un técnico externo, el tratamiento de la información debería concretarse en un contrato o acuerdo de encargo del tratamiento.

Barcelona, 29 de julio de 2021

Traducción Automática