IAI 6/2022

Informe complementario emitido a petición de la Comisión de Garantía del Derecho de Acceso a la Información Pública en relación con la petición de informe que un Departamento de la Generalidad habría formulado en la GAIP, en el marco de la sesión de mediación de la Reclamación (...).

La Comisión de Garantía del Derecho de Acceso a la Información Pública (GAIP) pide a la Autoridad Catalana de Protección de Datos (APDCAT) que emita un informe, en relación con la petición de informe que la administración autonómica habría formulado a la GAIP, en el marco de la sesión de mediación de la Reclamación (...).

En el acuerdo de mediación de 27 de enero de 2022, relativo a la reclamación (...), la persona reclamante y el Departamento, habrían acordado pedir un informe a la GAIP "sobre si es viable jurídicamente hacer una copia de un más de registro y sobre a qué datos de la copia procede que acceda una persona que tiene la condición de periodista."

Vista esta solicitud de dictamen en la GAIP, acordada en el acuerdo de mediación, la GAIP pide a la Autoridad que emita informe en relación con el acceso a los datos del Registro de Accesos del Palacio de la Generalitat, teniendo en cuenta que dicho Registro contiene datos de carácter personal. La GAIP solicita el parecer de la Autoridad para poder tenerlo en cuenta en la valoración jurídica del dictamen que emitirá la propia Comisión.

Analizada la solicitud, que se acompaña de una copia del acta de la sesión de mediación, y de la documentación del expediente correspondiente, y de acuerdo con el informe de la Asesoría Jurídica, se emite el siguiente informe:

Antecedentes

1. En fecha 23 de agosto de 2021, un ciudadano presentó un escrito al Departamento, en el que solicitaba conocer el control de acceso al Palacio de la Generalidad, en concreto:

> **"(…). El detalle de todas y cada una de las personas que han accedido al Palacio de la Generalidad desde el 1 de enero de 2021 hasta la actualidad. Solicito que para cada una de ellas se me indique: el número y la información de detalles del empleo de la persona que realiza la visita, la fecha de la visita, el número y cargo de la persona visitada en el complejo y la hora de entrada y la de salida al complejo. (…)."**

2. En fecha 5 de noviembre de 2021, el solicitante presentó reclamación ante la GAIP, dado que, según explica, no habría recibido la información solicitada. Según el reclamante, "Presidencia alega que no guarda tanto tiempo las datos y que sólo dispone de ellos para el último mes. En ese caso debería aplicar el acceso de forma parcial y entregar al menos ese último mes."

3. En fecha 29 de noviembre de 2021, la GAIP solicitó a esta Autoridad la emisión del informe previsto por el artículo 42.8 de la Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno, en relación con la Reclamación.

4. En fecha 12 de enero de 2022, la Autoridad envió a la GAIP el Informe IAI 83/2021, en el que concluye lo siguiente:

> **"La normativa de protección de datos no impide el acceso a la información relativa a visitas de personas pertenecientes a grupos de interés, ni a la información sobre visitas directamente relacionadas con la actividad pública de la Administración (visitas protocolarias, reuniones institucionales, etc).**
>
> **La información sobre visitas de personas que actúan en nombre y representación de personas jurídicas, con finalidades distintas de las actuaciones propias de los grupos de interés, se puede facilitar omitiendo la identidad de la persona concreta que las representa, salvo que se cuente con el consentimiento expreso de las personas afectadas o se trate de datos hechos manifiestamente públicos por estas personas.**
>
> **La normativa de protección de datos no habilitaría comunicar de forma generalizada la identidad de terceras personas físicas que actúan en nombre propio y que visiten las dependencias del Departamento.**
>
> **Sin perjuicio de la obligación de transparencia respecto a las agendas públicas de altos cargos o personal directivo y personal asimilado a subdirección general, tampoco parece justificado facilitar un acceso generalizado a la identidad de todos y cada uno de los trabajadores públicos que reciben visitas."**

5. Consta en el expediente copia del Acta de 26 de enero de 2022, de la sesión de mediación relativa a la Reclamación, así como copia del Acuerdo de mediación, de fecha 27 de enero de 2022, en el que las partes acuerdan pedir formalmente a la GAIP que se pronuncie jurídicamente a través de un Dictamen "sobre si es viable jurídicamente realizar una copia de un mes de registro y sobre a qué datos de la copia procede que acceda una persona que tiene la condición de periodista."

6. En la misma fecha de 26 de enero de 2022, el Departamento remite a la GAIP un escrito en el que solicita informe sobre "si procede bloquear los datos en caso de que se produzca una solicitud de acceso a la información pública."

7. En fecha 14 de febrero de 2022, el Departamento remite, a petición de la GAIP, la solicitud formal de dictamen en relación con los siguientes aspectos:

> **"Viabilidad jurídica o no de bloquear los datos de un tratamiento de datos sujeto a supresión automática en aplicación de lo que establece la Instrucción 1/1996 de la Agencia Española de Protección de Datos en base a una solicitud de acceso a la información pública, teniendo en cuenta que, de acuerdo con la normativa, la información se destruye de forma automática en el plazo de un mes desde su recogida.**

En este punto, se solicita el informe de la GAIP, sin perjuicio de que la controversia concreta sobre el fundamento para bloquear estos datos, cuya destrucción deriva de la Instrucción 1/1996, entendemos que corresponde determinarla 'Autoridad Catalana de Protección de Datos (APDCAT).

En el caso de dictaminar sobre la viabilidad del bloqueo, establecer qué datos de los disponibles en el tratamiento se pueden facilitar, teniendo en cuenta la finalidad de la recogida de los datos, y las consideraciones realizadas en el informe emitido por la APDCAT. ”

8. En fecha 22 de febrero de 2022, la GAIP solicita a esta Autoridad que emita informe sobre la cuestión planteada, a fin de poder tenerlo en cuenta en la valoración jurídica del dictamen que emitirá la GAIP.

Fundamentos Jurídicos

De conformidad con el artículo 1 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, la APDCAT es el organismo independiente que tiene por objeto garantizar, en el ámbito de las competencias de la Generalidad, los derechos a la protección de datos personales y de acceso a la información vinculada a ellos.

El artículo 42.8 de la Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno, que regula la reclamación contra las resoluciones en materia de acceso a la información pública, establece que si la denegación se ha fundamentado en la protección de datos personales, la Comisión debe emanar informe a la Autoridad Catalana de Protección de Datos, el cual debe ser emitido en el plazo de quince días.

En el caso que nos ocupa, la APDCAT emitió el informe IAI 83/2021, en relación con la Reclamación (...), y emite informe complementario, a petición de la GAIP, sobre las cuestiones planteadas por el Departamento en el procedimiento de mediación de la Reclamación, citada.

Este informe se emite exclusivamente en lo que se refiere a la valoración de la incidencia que el acceso solicitado puede tener respecto de la información personal de las personas afectadas (artículo 4.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo , de 27 de abril, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de los datos personales (en adelante, RGPD).

De acuerdo con el artículo 17.2 de la Ley 32/2010, este informe se publicará en la web de la Autoridad una vez notificado a las personas interesadas, previa anonimización de los datos de carácter personal.

II

La Reclamación (...), en relación con la que se emite este informe complementario, se interpone contra la denegación del acceso a información relativa al registro de personas que hubieran accedido

en el Palacio de la Generalidad desde el 1 de enero de 2021 hasta el momento de formular la solicitud (23 de agosto de 2021), en concreto, "el número y la información de detalles del empleo de la persona que realiza la visita, la fecha de la visita, el número y cargo de la persona visitada en el complejo y la hora de entrada y la de salida en el complejo."

Como recuerda esta Autoridad en el informe IAI 83/2021, emitido a petición de la GAIP en relación con la Reclamación (...), los datos de las personas físicas que han accedido al Palau de la Generalitat durante el periodo en el al que se refiere la solicitud, así como los datos de las personas que reciben la visita, son datos personales y quedan protegidos por los principios y garantías de la normativa de protección de datos.

Sin perjuicio de las consideraciones hechas en el Informe IAI 83/2021, a las que nos remitimos, en este informe es necesario analizar la cuestión planteada por el Departamento en la GAIP, sobre la que la GAIP pide el parecer de esta Autoridad, en concreto:

> **"Viabilidad jurídica o no de bloquear los datos de un tratamiento de datos sujeto a supresión automática en aplicación de lo que establece la Instrucción 1/1996 de la Agencia Española de Protección de Datos en base a una solicitud de acceso a la información pública, teniendo en cuenta que, de acuerdo con la normativa, la información se destruye de forma automática en el plazo de un mes desde su recogida.**
>
> **En este punto, se solicita el informe de la GAIP, sin perjuicio de que la controversia concreta sobre el fundamento para bloquear estos datos, cuya destrucción deriva de la Instrucción 1/1996, entendemos que corresponde determinarla 'Autoridad Catalana de Protección de Datos (APDCAT).**
>
> **(...)"**

Situado el objeto de informe en estos términos, es necesario partir de la base de que cualquier tratamiento de datos personales debe dar cumplimiento a los principios y garantías establecidos en la normativa (RGPD).

Según el artículo 5.1 RGPD: "Las datos personales serán: (...).

> **b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de modo incompatible con dichas finas; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de las datos personales con fines de archivo en interés público, fines de investigación científica e histórico o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad») ;" (…). e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de las datos personales; las datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente fines de archivo en interés público, fines de investigación científica o histórico o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento al objeto de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);**

(…).”

El responsable debe aplicar el principio de limitación del plazo de conservación, teniendo en cuenta la finalidad de que pueda tener un determinado tratamiento de datos personales, a fin de que el tratamiento no se alargue en el tiempo más allá de lo necesario para alcanzar la finalidad (art. 4.7 y art. 5.2 RGPD). Ello, sin perjuicio de la conservación, en su caso, para las ulteriores finalidades que resulten compatibles en los términos de la normativa de protección de datos.

Por tanto, de entrada, está claro que la conservación de los datos personales dependerá en cada caso de lo que sea necesario para dar cumplimiento a la finalidad del tratamiento.

En el marco de los principios mencionados de limitación del plazo de conservación y de limitación de la finalidad, el artículo 32 de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales (LOPDGDD), impone al responsable del tratamiento -en el caso que nos ocupa, el Departamento-, la obligación de bloqueo de los da

“1. El responsable del tratamiento estará obligado a bloquear las datos cuando proceda a su rectificación o supresión.

2. El bloqueo de las datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, salvo para la puesta a disposición de las datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

Transcurrido ese plazo deberá procederse a la destrucción de las datos.

3. Las datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.

(...)”.

Por tanto, el bloqueo es una obligación que el responsable debe aplicar necesariamente, y sólo con las excepciones previstas en la ley, cuando debe procederse a la rectificación o supresión de datos.

En base a esta obligación general de bloquear la información que debe ser objeto de supresión (según el plazo establecido para cada tratamiento), debe entenderse que la supresión no equivale, de entrada, a la destrucción física de la información.

Cabe decir que la obligación de bloqueo, prevista en la LOPDGDD con carácter general, admite algunas excepciones que la misma norma explicita (como, en relación con los tratamientos con finalidad de videovigilancia, ej. art. 22.3 LOPDGDD, o en relación con tratamiento de datos en sistemas de información de denuncias internas, ej.art.24.4 LOPDGDD). En estos casos, la norma explicita que no se aplica el bloqueo de la información, por tanto, se puede proceder a la destrucción física de la información, una vez cumplido el plazo de conservación.

Ahora bien, más allá de estas excepciones, debe entenderse que la obligación de bloqueo opera siempre que deba procederse a la supresión de información personal. Por tanto, en principio, también en relación con el caso que nos ocupa (supresión de datos del control de accesos del Departamento).

Como se recuerda en el Informe IAI 83/2021, según el informe del Departamento, de 29 de noviembre de 2021 (emitido a petición de la GAIP en relación con la Reclamación ...), la información que solicita el reclamante formaría parte del tratamiento "Control de presencia", incluido en el Registro de actividades del tratamiento (RAT) del Departamento.

Como se desprende de la información disponible (Acta de mediación de 26 de enero de 2022), el Departamento habría manifestado dudas "sobre si la propia solicitud de acceso a la información pública habilita el procedimiento de supresión de la destrucción automática de las datos, dado que deben bloquear una supresión de un procedimiento automatizado, es decir, que deben bloquearse datos que deberían haber sido suprimidos" (motivo por el que se solicita que se haga consulta a esta Autoridad) .

Como también se desprende de la información disponible (Acta de mediación de 26 de enero de 2022, y solicitud de Dictamen en la GAIP, de 14 de febrero de 2022), el Departamento considera que el período de conservación previsto para el tratamiento de datos del "Control de presencia", es de un mes, y que la obligación de destrucción efectiva de los datos en este período de un mes deriva de la "Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre archivos automatizados establecidos con la finalidad de controlar el acceso a los edificios", que se adjunta al expediente.

Así, el Departamento fundamenta la obligación de suprimir (destruir) los datos del control de accesos en un mes, en las previsiones de la norma 5 de la Instrucción 1/1996, que dispone que "Las datos de carácter personal deberán ser destruidos cuando haya transcurrido el plazo de un mes, contado a partir del momento en que fueron recabados."

Ahora bien, es necesario puntualizar de entrada que el establecimiento del plazo de conservación de la información en el caso que nos ocupa, corresponde al responsable, es decir, al propio Departamento.

Esta obligación de destrucción efectiva en el plazo de un mes, no parece que pueda fundamentarse en una norma (la Instrucción 1/1996 de la AEPD) que se dicta en base a una normativa (Ley orgánica 5/1992) previa en la normativa vigente en materia de protección de datos, y de rango inferior al LOPDDDD. Pero es que además esta Instrucción dictada por la Agencia Española de Protección de Datos no es de aplicación a las entidades que, de acuerdo con el artículo 156 del EAC forman parte del ámbito de actuación del 'APDCAT, como es el caso del Departamento reclamado.

Más allá de esto, es necesario tener en cuenta también lo que establece el registro de actividades de tratamiento del Departamento.

El artículo 30.1 del RGPD indica la información que debe contener el RAT, entre otros: "f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos; (…)."

El RAT del Departamento prevé, para el tratamiento "Control de presencia", la conservación por un período de "menos de un año". Por tanto, de entrada, y según el propio RAT del responsable, no parece que el plazo de conservación deba ser necesariamente de un mes.

Además, la Mesa de acceso y evaluación documental -TAAD- (Código 869 de la Serie documental "Registro de acceso de personas externas a dependencias administrativas"), de aplicación al "control del acceso de las personas a los centros de trabajo y dependencias administrativas", que prevé la destrucción total, y un plazo (que debería entenderse como máximo), de cuatro años.

En este punto es necesario hacer referencia a la Ley 10/2001, de 13 de julio, de archivos y documentos, que tiene por objeto "impulsar la gestión y garantizar la preservación de la documentación de Cataluña, tanto pública como privada, de acuerdo con sus valores, para ponerla al servicio de los intereses generales; establecer los derechos y deberes de quienes son titulares, así como de los ciudadanos en relación con la mencionada documentación, y regular el Sistema de Archivos de Cataluña." (art. 1 Ley 10/2001).

Según dispone el artículo 2 de la Ley 10/2001, a los efectos de esta Ley se entiende por:

> **"(…).**
>
> **h) Documentación en fase activa: la documentación administrativa que una unidad tramita o utiliza habitualmente en sus actividades. Portal Jurídico de Cataluña**
>
> **i) Documentación en fase semiactiva: la documentación administrativa que, concluida la tramitación ordinaria, no es utilizada de forma habitual por la unidad que la ha producido en su actividad.**
>
> **j) Documentación inactiva o histórica: la documentación administrativa que, concluida la vigencia administrativa inmediata, posee valores primordialmente de carácter cultural o informativo."**

A efectos de su interés, la documentación generada por el tratamiento de datos con finalidad de control de visitas y acceso a edificios públicos, se encontraría en fase activa o semiactiva, mientras el Departamento, como responsable, deba utilizar de forma habitual aquella información, o deba disponer de ellos puntualmente.

En concreto, teniendo en cuenta lo determinado por el propio Departamento (RAT), parece que la documentación del control de accesos podría encontrarse en fase activa o semiactiva durante un plazo máximo de un año. En cualquier caso, y dado que el RAT especifica un plazo de conservación por un período de "menos de un año", el período podría ser inferior al año, si así lo establece el Departamento.

A partir de que la fase activa o semiactiva haya concluido (plazo que, como hemos dicho, correspondería al plazo máximo de un año fijado por el Departamento), y teniendo en cuenta lo previsto en la citada TAAD, el responsable debería mantener igualmente la información , hasta completar el plazo máximo de cuatro años previsto en la TAAD.

Así, aunque, pasado el plazo máximo de un año fijado por el Departamento, ya no deba tratarse la información del control de accesos, debería conservarse igualmente hasta completar el plazo de 4 años mencionado. Es en este período (una vez superado el plazo de un máximo de un año, hasta completar el plazo de 4 años previsto en la TAAD para poder destruir la documentación), que operaría el bloqueo de los datos personales, en los términos del artículo

El bloqueo de los datos permitiría al responsable disponer de la información, únicamente si fuera necesario tratarlos para hacer frente a posibles responsabilidades.

En cualquier caso, de todo lo expuesto se desprende que el Departamento no estaría "obligado" a destruir la información del control de accesos por aplicación de la Instrucción 1/1996, como ha quedado dicho, ni esta destrucción efectiva de información debe hacerlo en el plazo de un mes. Por el contrario, la información puede tratarse hasta completar el plazo máximo de un año, y debería conservarse debidamente bloqueada, hasta completar el plazo de 4 año, me

III

El artículo 32 de la LOPDDDD define el deber de bloqueo:

> **"1. El responsable del tratamiento estará obligado a bloquear las datos cuando proceda a su rectificación o supresión.**
> **2. El bloqueo de las datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, salvo para la puesta a disposición de las datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de las datos.**
> **3. Las datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior. (...)"**

Así pues, una vez aplicado el bloqueo, el artículo 32.2 de la LOPDDDD limita el tratamiento de los datos bloqueados a unos supuestos contraídos: la puesta a disposición de los datos a los jueces y tribunales, al Ministerio Fiscal oa las administraciones públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento en tanto no hayan prescrito.

Esta previsión normativa es ciertamente restrictiva en relación a los supuestos por los que la información bloqueada puede ser objeto de tratamiento.

Ahora bien, más allá de la literalidad del artículo 32.2 LOPDGDD, que establece una lista cerrada respecto a los posibles destinatarios de la información personal bloqueada y concreta la finalidad del bloqueo en la exigencia de responsabilidades derivadas del tratamiento, no parece posible denegar el acceso a datos bloqueados, por ejemplo, por parte de una persona afectada en ejercicio del derecho de acceso a la propia información personal (art. 15 RGPD).

Como recuerda esta Autoridad (informe CNS 76/2016), puede resultar lícito el tratamiento por parte de un responsable de determinados datos personales bloqueados, con el fin de cumplir una determinada obligación legal, por ejemplo, permitir el ejercicio de un derecho por parte de una determinada persona. Así lo ha reconocido también la Agencia Española de Protección de Datos en diversas resoluciones en relación a esta cuestión (entre otras, Resoluciones 00665/2021, 00532/2020, o 00484/2021).

Si bien en caso de que nos ocupa no es el titular de la información personal quien pide acceder al control de visitas del Departamento en ejercicio del derecho de acceso previsto en el artículo 15 RGPD, sino un tercero ajeno, en coherencia con el que se ha expuesto, el bloqueo de información personal tampoco debería despejar de contenido la posibilidad de ejercer otros derechos, como el derecho de acceso a información pública, en los términos de la legislación de transparencia. Especialmente si, como en el caso que nos ocupa, se han bloqueado los datos en un momento anterior al plazo que se deriva del registro de actividades del tratamiento del responsable.

Cuando se ejerce este derecho, obviamente no podrá exigirse a la Administración requerida facilitar información de la que no dispone. Como ya se hizo conveniente en el Informe IAI 83/2021, en caso de que nos ocupa el Departamento no debe facilitar, de hecho no puede aunque quiera, la información del control de accesos que ya haya eliminado.

Ahora bien, la información que esté bloqueada, si bien está sometida a un estricto régimen de acceso (art. 32 LOPDGDD), no ha sido todavía eliminada.

La comunicación de datos bloqueados tendría por finalidad cumplir con una obligación de la entidad responsable, fundamentada en la Constitución (art. 105.b) CE) y en la LTC. Esta atención de las responsabilidades del Departamento en esta materia, parece que debería tener cabida en los fines para los que el artículo 32 LOPDGDD prevé que se pueden utilizar los datos bloqueados.

Así, el acceso a determinada información personal bloqueada del control de accesos al Departamento (en los términos ya expuestos en el informe IAI 83/2021), podría quedar justificado y habilitado por el ejercicio del derecho de acceso a información pública por parte de un ciudadano, por un lado, y por la obligación del responsable de atender este derecho, por otro, respecto a la información pública que tiene en su poder.

Desde la perspectiva de la normativa de protección de datos, el tratamiento, en concreto, la comunicación de determinados datos del control de accesos a un ciudadano que ejerce el derecho de acceso a información pública, quedaría habilitado por el artículo 6.1. c) del RGPD, según el cual el tratamiento es lícito si es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento -en este caso dar cumplimiento a la legislación de transparencia-, sin que el bloqueo de la información pueda impedir el ejercicio de ese derecho.

Por todo lo expuesto, el bloqueo de información del Registro de visitas al Palacio de la Generalidad (control de accesos), del que dispondría el Departamento, se considera viable y ajustado a la normativa de protección de datos, en los términos expuestos en este informe.

IV

Dada la respuesta afirmativa a la primera cuestión planteada sobre la viabilidad jurídica del bloqueo en el caso examinado, cabe referirse a la siguiente cuestión planteada por el Departamento enviado a la GAIP y que ésta traslada a la Autoridad:

> **"En el caso de dictaminar sobre la viabilidad del bloqueo, establecer qué datos de los disponibles en el tratamiento se pueden facilitar, teniendo en cuenta la finalidad de la recogida de los datos, y las consideraciones realizadas en el informe emitido por la APDCAT ."**

De entrada, como se recuerda en el Fundamento Jurídico III del Informe IAI 83/2021, según constaba en el expediente correspondiente, la persona reclamante solicitaba conocer "el número y la información de detalles del empleo de la persona que realiza la visita, la fecha de la visita, el número y cargo de la persona visitada en el complejo ya hora de entrada y la de salida del complejo (...)."

Según consta en el punto tercero del Acuerdo de mediación de 27 de enero de 2022, "Las partes reconocen el derecho de la persona reclamante a volver a pedir formalmente la misma información sobre el Registro (...), pero de un alcance temporal diferente (...)."

Teniendo en cuenta esto, hacemos notar que esta Autoridad ya se pronunció sobre el acceso a los datos solicitados, en el Informe IAI 83/2021. A los efectos que interesan, cabe recordar que el acceso a la información pública solicitada debe tener diferente respuesta en diferentes supuestos analizados y en función de cuáles sean los colectivos o personas físicas afectadas (grupos de interés, personas físicas representantes) de personas jurídicas, personas físicas que actúan en nombre propio, etc.), en aplicación de la propia legislación de transparencia y de la normativa de protección de datos.

En este sentido, nos remitimos a las consideraciones de los FFJJ IV a VI del Informe IAI 83/2021, así como a las conclusiones de dicho informe:

> **"La normativa de protección de datos no impide el acceso a la información relativa a visitas de personas pertenecientes a grupos de interés, ni a la información sobre visitas directamente relacionadas con la actividad pública de la Administración (visitas protocolarias, reuniones institucionales, etc).**
>
> **La información sobre visitas de personas que actúan en nombre y representación de personas jurídicas, con finalidades distintas de las actuaciones propias de los grupos de interés, se puede facilitar omitiendo la identidad de la persona concreta que las representa, salvo que se cuente con el consentimiento expreso de las personas afectadas o se trate de datos hechos manifiestamente públicos por estas personas.**
>
> **La normativa de protección de datos no habilitaría comunicar de forma generalizada la identidad de terceras personas físicas que actúan en nombre propio y que visiten las dependencias del Departamento.**
>
> **Sin perjuicio de la obligación de transparencia respecto a las agendas públicas de altos cargos o personal directivo y personal asimilado a subdirección general, tampoco parece justificado**

facilitar un acceso generalizado a la identidad de todos y cada uno de los trabajadores públicos que reciben visitas."

Más allá de reiterar estas conclusiones, que responden a la pregunta formulada, hacemos notar que, según el Acta de la sesión de mediación de 26 de enero de 2022, las personas representantes del Departamento habrían insistido en que: "la finalidad concreta es saber quien hay y no indica qué persona entra ya quien va a ver." Según la propia Acta, el Departamento insiste en que "el control del registro se realiza exclusivamente por temas de seguridad y para saber quién hay en el Departamento y quizás no se puede saber a quién se va a ver."

Al respecto, cabe apuntar que consta en el expediente enviado a esta Autoridad copia del Listado de Control de Visitas, que incluye los campos que recogería el Departamento en el control de accesos. Según este listado que aporta el propio Departamento, los campos son los siguientes:

"Visita: Estado. Fecha Inicio. Fecha Fin. Sede/Deleg. Observaciones visita. Visitante: Nombre. Apellidos. DNI. Empresa visitante. Empleado: Nombre Empleado. Apellidos Empleado. Departamento."

Parece claro, pues, que el Departamento sí dispondría de información sobre la persona que realiza la visita, y sobre la persona visitada. Esto, sin perjuicio de que la finalidad del tratamiento sea una finalidad de seguridad que, como ya quedó expuesto en el Informe IAI 83/2021 (FJ II), tampoco es relevante a la hora de determinar qué es información pública a los efectos del artículo 2.b) LTC.

En cualquier caso, vistos los campos informativos que, por la información disponible, recoge el listado de control de visitas, podrá facilitarse la información en atención a las consideraciones ya hechas en dicho informe.

Así, por ejemplo, en caso de que el Departamento disponga de información sobre personas físicas que actúan en nombre y representación de personas jurídicas, como se recuerda en el FJ VI del Informe IAI 83/2021, en determinados casos será pertinente omitir la identidad de estas personas físicas, e indicar sólo "la empresa visitante".

Asimismo, por aplicación del principio de minimización, según el cual los datos que se tratan deben ser adecuados, pertinentes y limitados a lo necesario en relación con las finalidades del tratamiento (art. 5.1.c) RGPD), recuerda que no sería pertinente comunicar el DNI de las personas que visitan el Departamento, que se recoge en el citado Listado de Control de Visitas.

Finalmente, en lo que se refiere al campo "Observaciones visita", parece que podría referirse al motivo de la visita.

Al respecto, en síntesis, y sin perjuicio de remitirnos a las consideraciones del Informe IAI 83/2021, puede apuntarse que, salvo las visitas de personas pertenecientes a grupos de interés o visitas directamente relacionadas con la actividad pública de la Administración (visitas protocolarias, reuniones institucionales...) o la referida a representantes de personas jurídicas, no parece que la normativa de protección de datos habilite a facilitar este tipo de información sobre los motivos de la visita, de forma generalizada.

Por todo ello, se realizan las siguientes conclusiones,

Conclusión

Desde la perspectiva de la normativa de protección de datos, resulta viable mantener la información del registro de accesos al Departamento debidamente bloqueada, en base a la obligación general de bloqueo del artículo 32 del LOPDDDD una vez la fase activa o semiactiva haya concluido (en el plazo máximo de un año fijado por el RAT). El Departamento debería mantener la información bloqueada, hasta completar el plazo máximo de cuatro años previsto en la TAA

El acceso a la información pública bloqueada debe tener diferente respuesta en función de cuáles sean los colectivos o personas físicas afectadas (grupos de interés, personas físicas representantes de personas jurídicas, personas físicas que actúan en nombre propio, etc), en aplicación de la legislación de transparencia y de la normativa de protección de datos. Nos remitimos al respecto a los fundamentos jurídicos IV a VI y las conclusiones del Informe IAI 83/2021 de esta Autoridad.

Barcelona, 24 de marzo de 2022