- **Expediente nº.: RR/00261/2023**

IMI Reference: A56 78728- Case Register 89995

- RESOLUCIÓN DE RECURSO DE REPOSICIÓN

Examinado el recurso de reposición interpuesto por GLOVOAPP23, S.A. (en lo sucesivo, la parte recurrente) contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos de fecha 7 de marzo de 2023, y en base a los siguientes

HECHOS

PRIMERO: Con fecha 7 de marzo de 2023, se dictó resolución por la Directora de la Agencia Española de Protección de Datos en el expediente PS/00209/2022, en virtud de la cual se decidía:

- DIRIGIR a GLOVOAPP23, S.A., con NIF A66362906, anteriormente GLOVOAPP23, S.L., con NIF B66362906, un apercibimiento, por una infracción del Artículo 13 del RGPD, tipificada en el Artículo 83.5 del RGPD, por no informar debidamente a los repartidores que, al utilizar el sistema "excellence score", se adoptaban decisiones automatizadas de las reguladas en el artículo 22 del RGPD.

- IMPONER a GLOVOAPP23, S.A., con NIF A66362906, anteriormente GLOVOAPP23, S.L., con NIF B66362906, una multa de 550.000 € (quinientos cincuenta mil euros), por la infracción de los Artículos 25 y 32 del RGPD, tipificadas en el Artículo 83.4 del RGPD, porque el sistema utilizado para la gestión de permisos de acceso a los datos de los repartidores permitía el acceso a datos no necesarios para el trabajo de los usuarios.

Dicha resolución, que fue notificada a la parte recurrente en fecha 17 de marzo de 2023, fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), y supletoriamente en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), en materia de tramitación de procedimientos sancionadores.

SEGUNDO: La parte recurrente ha presentado en fecha 17 de abril de 2023, en esta Agencia Española de Protección de Datos, recurso de reposición, en el que no se controvierten los hechos probados de la resolución del procedimiento sancionador objeto del presente recurso, por lo que aquéllos se consideran hechos probados de la presente resolución de recurso de reposición.

FUNDAMENTOS DE DERECHO

I

Competencia

Es competente para resolver el presente recurso la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo LPACAP) y el artículo 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

II

Contestación a las alegaciones presentadas

En relación con las manifestaciones efectuadas por la parte recurrente, se procede a dar respuesta a las mismas según el orden por ella expuesto:

PRIMERO.- INEXISTENCIA DE INFRACCIÓN LEVE DEL ARTÍCULO 13 DEL RGPD E INEXISTENCIA DE INFRACCIÓN GRAVE DE LOS ARTÍCULOS 25 Y 32 DEL RGPD

1.1. Ausencia de decisiones automatizadas a las que se refiere el artículo 22 RGPD en el sistema “excellence score”

Alega la parte recurrente que “de ningún modo se puede considerar a Glovo autor de la infracción leve del artículo 13 RGPD, en su apartado 2.f) consistente en no informar sobre las decisiones individuales automatizadas basadas en tratamientos automatizados que presuntamente Glovo tomaba respecto a los repartidores cuando daba acceso preferencial para la reserva de una franja horaria determinada a partir de la valoración del “excellence score” del repartidor, simplemente porque no existían tales decisiones”.

Y que lo que existía era un proceso automatizado basado en parámetros definidos manualmente por Glovo y aceptados por el repartidor que permitían holgadamente la “participación humana”.

Alega que en la Resolución Sancionadora la AEPD hace referencia al documento del ya extinto Grupo de Trabajo del Artículo 29 “*Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*” para justificar la existencia de tales decisiones individuales automatizadas basadas en tratamientos automatizados, pero que la AEPD ha pasado por alto que en esas mismas directrices se define cómo debe ser la “participación humana” para que el tratamiento no pueda subsumirse en la definición de “decisión basada únicamente en el tratamiento automatizado” recogida por el artículo 22 del RGPD. A saber:

“Para ser considerada como participación humana, el responsable del tratamiento debe garantizar que cualquier supervisión de la decisión sea significativa**,** en vez de ser únicamente un gesto simbólico. Debe llevarse a cabo por parte de una persona autorizada y competente para modificar la decisión. Como parte del análisis, debe tener en cuenta todos los datos pertinentes.” (el destacado es de Glovo)

La parte recurrente entiende que ha quedado acreditado que el número de intervenciones humanas que se produjeron en el sistema “excellence score” constituye “claramente una supervisión “significativa” alterando la decisión que inicialmente

hubiera tomada el sistema “excellence score” por parte de operadores expresamente autorizados a ello”

Al respecto, esta Agencia desea reiterar lo ya expuesto en la citada Resolución Sancionadora objeto del presente recurso.

En primer lugar, defender la tesis de que la parte recurrente aplicaba una tabla de franjas horarias “acordadas por las partes”, que ejecutaba una decisión “adoptada por las partes de mutuo acuerdo” y que daba entrada a la franja horaria según un orden previamente establecido “en función de las preferencias de las partes” resulta, cuanto menos, sorprendente, por cuanto aún en el hipotético caso de que los trabajadores aceptaran la utilización del sistema “excellence score” para poder participar en la plataforma y conocieran la existencia de una tabla de franjas horarias, debieron ser informados de que se tomaban decisiones automatizadas de las contempladas en el art. 22 del RGPD, en los términos recogidos en el art. 13 del RGPD.

En segundo lugar, las citadas *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679* disponen: “*Las decisiones basadas únicamente en el tratamiento automatizado representan la capacidad de tomar decisiones por medios tecnológicos sin la participación del ser humano*”.

Es decir, la toma de una decisión automatizada no consiste en un mero proceso automatizado, como podría ser un sistema de expedición de pedidos automático o de recepción de mercancías, sino que hace referencia a la capacidad de tomar decisiones por medios tecnológicos. El uso de la tecnología para tomar decisiones que afectan a personas y que requieren el tratamiento de datos personales supone un mayor riesgo para los derechos y libertades de los interesados, pues el algoritmo puede tomar decisiones erróneas, sesgadas o injustas. Por ello el RGPD fija las garantías que deben adoptarse en el uso de algoritmos que toman decisiones debido al mayor riesgo que comportan, entre ellas se impone al responsable un deber de transparencia.

En el punto IV de las citadas Directrices se dice:

“El artículo 22, apartado 1, se refiere a las decisiones «basadas únicamente» en el tratamiento automatizado. Esto quiere decir que no hay participación humana en el proceso de decisión.

Ejemplo
Un proceso automatizado produce lo que es, en realidad, una recomendación relativa al interesado. Si un ser humano revisa y tiene en cuenta otros factores para tomar la decisión final, dicha decisión no estará «basada únicamente» en el tratamiento automatizado.

El responsable del tratamiento no puede obviar las disposiciones del artículo 22 inventándose una participación humana. Por ejemplo, si alguien aplica de forma rutinaria perfiles generados automáticamente a personas sin que ello tenga influencia real alguna en el resultado, esto seguiría siendo una decisión basada únicamente en el tratamiento automatizado.

Para ser considerada como participación humana, el responsable del tratamiento debe garantizar que cualquier supervisión de la decisión sea significativa, en vez de ser únicamente un gesto simbólico. Debe llevarse a cabo por parte de una persona autorizada y competente para modificar la decisión. Como parte del análisis, debe tener en cuenta todos los datos pertinentes.

Como parte de la EIPD, el responsable del tratamiento debe identificar y registrar el grado de participación humana en el proceso de toma de decisiones y en qué punto se produce esta".

En el presente caso, esta Agencia entiende que es el sistema el que adoptaba la decisión sobre en qué orden se permitía acceder a unos repartidores determinados para la reserva de una franja horaria concreta, independientemente de que era la parte recurrente como responsable de tratamiento quien introducía los parámetros necesarios en el Sistema para que pudiera adoptar tal decisión.

La decisión sobre el orden en que se permitía acceder a los repartidores a las franjas horarias era adoptada por la aplicación, sin intervención humana de ningún tipo. Únicamente se producía una intervención humana en aquellos casos en que los repartidores reclamaban, pero si no había reclamación, no había intervención humana que modificara dicha decisión ni supervisión alguna de tal decisión.

El hecho de que se hubiera producido un número determinado de intervenciones humanas no obsta a que la decisión sobre el acceso a las franjas horarias en cuestión ha sido adoptada por la aplicación sin ninguna intervención humana por su parte, sobre todo si se tiene en cuenta que la intervención humana no se producía en todos los casos y que ésta se realizaba tras una reclamación de los interesados, lo que daría cumplimiento a la obligación del responsable de garantizar el derecho de los interesados a obtener intervención humana, como se recoge en el artículo 22.3 del RGPD, al disponer: "*En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión*", y en el considerando 71: "(…) *Sin embargo, se deben permitir las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles, si lo autoriza expresamente el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento, incluso con fines de control y prevención del fraude y la evasión fiscal, realizada de conformidad con las reglamentaciones, normas y recomendaciones de las instituciones de la Unión o de los órganos de supervisión nacionales y para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento, o necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable del tratamiento, o en los casos en los que el interesado haya dado su consentimiento explícito. En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión (…)".* Pero la adopción de este sistema de garantías no exime al responsable de dar cumplimiento a los deberes de información recogidos en el artículo 13.2.f) del RGPD.

En tercer lugar, esta Agencia entiende que era el Sistema el que conformaba los bloques de repartidores y les asignaba un orden de prioridad a la hora de poder seleccionar una determinada franja horaria, en base al "*excellence score*".

Esta selección se realizaba sin intervención humana, esto es, de forma automatizada, tal como se explicó anteriormente. Con independencia de que pueda haber intervención humana en todas las fases del proceso, la determinación de los bloques de repartidores y su prioridad a la hora de seleccionar una franja horaria, la realizaba el Sistema. La intervención humana era una posibilidad que existía para realizar acciones concretas y que podían modificar la decisión tomada por el Sistema, pero ello no obsta a que la decisión de qué prioridad se le asignaba a un repartidor se estaba tomando de forma automatizada.

En cuarto lugar, en el informe pericial aportado como DOCUMENTO 2 de las alegaciones al acuerdo de inicio del procedimiento sancionador, se analiza una muestra de operaciones representativa del sistema *excellence score* para acreditar la inexistencia de decisiones individuales automatizadas, en los meses febrero y marzo de 2020, fechas en las que tuvo lugar la inspección de la AEPD, en el que se concluye:

"De los resultados anteriores se deduce una clara intervención humana en la toma de decisiones al respecto del acceso a los repartidores a la reserva de franjas horarias, llegando incluso en algunos casos a cerca del 40% de las operaciones totales analizadas."

El citado informe detalla que "entre las fechas 20 de marzo de 2020 y 1 de abril de 2020 hubo un total de 16.175 entradas de registro, de las cuales el 38,6% fueron intervenciones manuales correspondientes a acciones de "kickout" o expulsión manual de repartidores de la franja horaria reservada. Estas acciones fueron realizadas por 29 operadores humanos diferentes".

Y que "en una muestra de una semana (del 24 de marzo de 2020 al 1 de abril de 2020) hubo hasta 13 incrementos manuales de la capacidad de las franjas horarias, realizados por 6 operadores humanos diferentes".

Pero esta Agencia desea señalar que las *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679* indican que:

"*El artículo 22, apartado 1, se refiere a las decisiones «basadas únicamente» en el tratamiento automatizado. Esto quiere decir que no hay participación humana en el proceso de decisión. (…)*
(…)

Para ser considerada como participación humana, el responsable del tratamiento debe garantizar que cualquier supervisión de la decisión sea significativa, en vez de ser únicamente un gesto simbólico. Debe llevarse a cabo por parte de una persona autorizada y competente para modificar la decisión. Como parte del análisis, debe tener en cuenta todos los datos pertinentes.

Como parte de la EIPD, el responsable del tratamiento debe identificar y registrar el grado de participación humana en el proceso de toma de decisiones y en qué punto se produce esta".

En el presente caso, el hecho de que hubiera existido un número determinado de intervenciones humanas no implica que el Sistema no estuviera tomando decisiones automatizadas. De hecho, el artículo 22 del RGPD establece que, en los casos en que el tratamiento es necesario para la ejecución del contrato (como en el presente supuesto), "*el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión*". Por tanto, la posibilidad de que exista intervención humana en caso de adoptar decisiones automatizadas es, incluso, una obligación impuesta al responsable de tratamiento, quien debe garantizarle esa posibilidad a los afectados por dichas decisiones.

En cualquier caso, la parte recurrente mediante la utilización del "*excellence score*" estaba tomando decisiones automatizadas de las del artículo 22 del RGPD sin informar de ello (incluso negándolo) en los documentos pertinentes, infringiendo lo dispuesto en el artículo 13 del RGPD.

En quinto lugar, esta Agencia desea señalar que el artículo 22 del RGPD establece: "*Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar*". Es decir, que las decisiones individuales automatizadas reguladas en el artículo 22 son aquellas que se basan únicamente en el tratamiento automatizado y que produzcan efectos jurídicos en los interesados o les afecte significativamente de modo similar.

En este sentido, esta Agencia entiende que el "*excellence score*" producía efectos jurídicos en los interesados toda vez que les asignaba una prioridad para poder acceder a la reserva de horas de una franja determinada, lo cual repercutía directamente en su trabajo y sus ingresos. El hecho de que pudiera existir una intervención manual, ya se ha explicado anteriormente, no obsta que en el presente caso se estuvieran tomando decisiones individuales automatizadas.

Por tanto, esta Agencia insiste en que GLOVOAPP sí que estaba realizando decisiones individuales automatizadas y, por tanto, debió informar debidamente a los repartidores de tal situación.

El considerando 71 del RGPD dispone:

"(71) El interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar, como la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna. Este tipo de tratamiento incluye la elaboración de perfiles consistente en cualquier forma de tratamiento automatizado de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar

o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Sin embargo, se deben permitir las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles, si lo autoriza expresamente el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento, incluso con fines de control y prevención del fraude y la evasión fiscal, realizada de conformidad con las reglamentaciones, normas y recomendaciones de las instituciones de la Unión o de los órganos de supervisión nacionales y para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento, o necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable del tratamiento, o en los casos en los que el interesado haya dado su consentimiento explícito. En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión. Tal medida no debe afectar a un menor".

Las ya citadas *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679* explican:

"(…)
En resumen, el artículo 22 dispone lo siguiente:

i) como norma, existe la prohibición general de tomar decisiones individuales basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos o efectos significativamente similares;
ii) existen excepciones a esta norma;
iii) cuando se aplique una de estas excepciones, deberán existir medidas en vigor para garantizar los derechos y libertades del interesado, así como sus intereses legítimos.

Esta interpretación refuerza la idea de que sea el interesado quien tenga el control sobre sus datos personales, lo cual se corresponde con los principios fundamentales del RGPD. Interpretar el artículo 22 como una prohibición en vez de como un derecho que debe invocarse significa que las personas están protegidas automáticamente frente a las posibles consecuencias que pueda tener este tipo de tratamiento. La redacción del artículo sugiere que esta es la intención, y se ve apoyada por el considerando 71, que establece lo siguiente:

«Sin embargo, se deben permitir las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles, si lo autoriza expresamente el Derecho de la Unión o de los Estados miembros [...], o necesario para la conclusión o ejecución de un contrato [...], o en los casos en los que el interesado haya dado su consentimiento explícito».

Esto implica que el tratamiento previsto en el artículo 22, apartado 1, no se permite por lo general.

No obstante, la prohibición del artículo 22, apartado 1, solo se aplica en circunstancias específicas cuando una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, produce efectos jurídicos o afecta significativamente

de forma similar a alguien, como se explica más adelante en las directrices. Incluso en estos casos, existen excepciones definidas que permiten realizar dicho tratamiento.

Las medidas de protección obligatorias, descritas en más detalle a continuación, incluyen el derecho a ser informado (previsto en los artículos 13 y 14 —información específicamente significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas para el interesado—) y garantías, como el derecho a obtener intervención humana y el derecho a impugnar la decisión (previstos en el artículo 22, apartado 3).

Cualquier tratamiento que entrañe probablemente un alto riesgo para los interesados exige que el responsable del mismo lleve a cabo una evaluación de impacto relativa a la protección de datos (EIPD). Además de abordar cualquier otro riesgo relacionado con el tratamiento, una EIPD puede ser especialmente útil para aquellos responsables del tratamiento que no estén seguros de si sus actividades propuestas se ajustan a la definición del artículo 22, apartado 1, y, en caso de que una excepción identificada las permita, de qué medidas de protección deben aplicarse. (…)"

Es decir, en principio, el RGPD prohíbe la toma de decisiones individuales basadas únicamente en el tratamiento automatizado, que produzcan efectos jurídicos en él o que le afecte significativamente, como en este caso, dado que la prioridad con que un repartidor ingresa en una determinada franja horaria, o no, le afecta directamente en sus ingresos. Por tal motivo se refuerza en estos casos el deber de transparencia, a fin de que el interesado conozca que se toman decisiones automatizadas y sus efectos.

En sexto lugar, tal como ha quedado acreditado en el presente procedimiento, el sistema "excellence score" es la puntuación asignada a los repartidores, en base a, entre otros, los siguientes datos:

a. el número de pedidos realizados en franjas horarias de alta demanda en los últimos 28 días,
b. el feedback de las tiendas en los últimos 50 pedidos, que puede ser positivo, negativo o no valorado,
c. el feedback de los usuarios en los últimos 50 pedidos, que puede ser positivo, negativo o no valorado,
d. pedidos rechazados o reasignados en los últimos 50 pedidos, aunque, en España, la reasignación no penaliza,
e. histórico de pedidos desde el inicio de la colaboración.

Esta puntuación se calcula de forma automática, sin intervención humana alguna, en base a los citados parámetros. Si bien es cierto que los valores utilizados para calcular la *excellence score* podrían ser modificados manualmente, solamente se realizaría en el caso de que un repartidor presente una queja, normalmente a través de facturación.

Volviendo a la cuestión que nos ocupa, para poder decidir qué repartidores trabajarían en una determinada franja horaria, el procedimiento que seguía GLOVOAPP era el siguiente:

1) Se calculaba (de forma automatizada) el número máximo de repartidores que serían necesarios para una determinada franja horaria en un día determinado.

2) Se seleccionaba (de forma automatizada) a todos los repartidores registrados en una ciudad o área de funcionamiento de la app.
3) Se ordenaba a estos repartidores (de forma automatizada) según su *Excellence Score* (calculado también de forma automatizada).
4) Dos veces por semana (lunes y jueves) se enviaba una notificación (de forma automatizada) a cada repartidor informando que ya tenía disponible la selección de franjas horarias de ciertos días de la semana (los lunes podían reservar las franjas horarias de jueves, viernes, sábado y domingo; y los jueves podían reservar las franjas horarias de lunes, martes, miércoles de la siguiente semana), siguiendo un orden decreciente en base a la ordenación anterior.

Por supuesto que en cada una de estas fases podía existir intervención humana para corregir algunas cuestiones puntuales (y previa queja), pero la realidad era que todo el proceso se realizaba de forma automatizada por lo que la decisión sobre qué repartidores accedían o no a una determinada franja horaria y en qué orden, era una decisión automatizada.

Además, esta decisión automatizada producía efectos jurídicos sobre el interesado (en este caso, los repartidores) toda vez que la posibilidad de acceder o no a una determinada franja horaria le afectaba directamente en sus ingresos.

Por tanto, en el presente caso, esta Agencia considera que, en el presente caso, GLOVOAPP estaba tomando decisiones automatizadas de las referidas en el artículo 22 del RGPD, por lo que tal situación debía ser informada a los repartidores en esos términos y GLOVOAPP infringió lo dispuesto por el artículo 13 del RGPD al no hacerlo.

Por todo lo expuesto, se desestima la presente alegación.

Asimismo, la parte recurrente alega que, en caso de finalmente considerarse que Glovo realizaba decisiones individuales automatizadas con el uso del sistema “excellence score”, la propia AEPD ya reconoce que éstas ya eran informadas a los repartidores a través de vídeos y del blog, tal como se indica expresamente en la página 128 de la Resolución Sancionadora.

Al respecto, esta Agencia desea señalar que es cierto que se informaba sobre la existencia del “excellence score”, pero no se señalaba que su utilización implicara la existencia de decisiones automatizadas, tal como exige el RGPD en su artículo 13.2.f).

Por último, el hecho de que se proporcionara información sobre el “excellence score” a los repartidores a través de otros medios distintos a los contratos entre la parte recurrente y los repartidores ya ha sido tenido en cuenta por esta Agencia para sustituir una posible sanción de multa por dirigir un apercibimiento, en los términos del artículo 58.2.b) del RGPD.

Por todo lo expuesto, se desestima la presente alegación.

1.2. Ausencia de acceso indiscriminado a datos personales de los repartidores y existencia de responsabilidad proactiva de Glovo

Alega la parte recurrente que de ningún modo tampoco se puede considerar a Glovo autor de la infracción grave de los artículos 25 y 32 RGPD consistente en la existencia de un acceso indiscriminado a los datos de los repartidores.

Y que se ha demostrado holgadamente que Glovo tenía claramente definidos en su organización perfiles de usuario que, a su vez, posibilitaban el acceso a aquellos datos de repartidores únicamente necesarios para cumplir con las finalidades de tratamiento definidas en cada momento, lo cual iba acorde con la estructura organizativa que Glovo ha ido ostentado a lo largo del tiempo desde su constitución.

Asimismo, alega la parte recurrente que la Resolución Sancionadora "critica erróneamente a Glovo por no adoptar una actitud proactiva a la hora de cumplir con los principios y obligaciones que establece el RGPD, toda vez que presuntamente no realizó un análisis previo al tratamiento de datos de repartidores en el que se analizaran las posibles implicaciones para sus derechos y libertades".

A este respecto, la parte recurrente, además del DOCUMENTO 30 que obra en el expediente donde a su entender se realizó un análisis del tratamiento de los riesgos que el mismo conllevaba para los derechos y libertades de los repartidores, trae a colación el análisis de riesgos transversal que Glovo ya había realizado con la ayuda de sus asesores externos ******EMPRESA.1*** (DOCUMENTO 1), aplicable en general a todos los tratamientos realizados por Glovo y que concluyó no suponían un riesgo especial para los derechos y libertades de los interesados.

La parte recurrente entiende que ello demuestra que Glovo sí ha tenido en cuenta los principios de protección de datos y los riesgos que sus tratamientos pueden generar a todos los interesados (repartidores incluidos), ello acorde con el principio de responsabilidad activa que exige el RGPD y que erróneamente la AEPD tilda a Glovo de no respetar.

En relación con este análisis, la parte recurrente precisa que no se ha aportado hasta este momento puesto que se trataba de un análisis transversal a todos los tratamientos, y que el mismo no está únicamente dirigido a tratamiento de datos de repartidores.

Al respecto, esta Agencia desea reiterar lo ya expuesto en la citada Resolución Sancionadora objeto del presente recurso.

En primer lugar, el literal del apartado 2 del artículo 25 del RGPD es el siguiente:

"2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas".

Esto es, que la obligación de aplicar las medidas apropiadas para garantizar que solo sean objeto de tratamiento los datos personales necesarios para cada uno de los fines específicos del tratamiento, se aplica no solo a la accesibilidad de los datos sino también a la cantidad de datos personales recogidos, a la extensión de su tratamiento y a su plazo de conservación.

Y que, en particular, tales medidas deben garantizar que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas. Esto es, que tales medidas deben garantizar lo anteriormente expuesto, pero no únicamente eso.

Esta Agencia insiste en que cuando el RGPD se refiere a las medidas que garanticen los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas, utiliza la coletilla “en particular”. Esto significa que impedir el acceso de forma indiscriminada a los datos de los repartidores es una de las obligaciones a las que hace referencia el RGPD, pero no es la única. De hecho, la primera obligación a la que hace referencia el artículo 25.2 del RGPD es aplicar las medidas apropiadas para garantizar que, por defecto, solo se traten los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. O dicho de otra manera, que no se traten datos que no sean los estrictamente necesarios para cada finalidad para la que se traten.

En el presente caso, se estaban tratando datos de repartidores de países que no era necesario tratar para realizar el seguimiento de esos repartidores como consecuencia de la falta de previsión en el diseño de medidas adecuadas para garantizar el cumplimiento del principio de minimización, así como de la ausencia de medidas apropiadas para garantizar que, por defecto, sólo se traten los datos necesarios. Por tanto, se incumple el artículo 25 del RGPD.

Lo mismo puede decirse del artículo 32 del RGPD, toda vez que las medidas técnicas y organizativas aplicadas no garantizaban un nivel de seguridad adecuado al riesgo, dado que el sistema permitía a los usuarios el acceso a datos de repartidores que no era necesario que trataran para la finalidad que se usaban.

En segundo lugar, esta Agencia desea recordar el concepto de responsabilidad proactiva, regulado en el artículo apartado 2 del artículo 5 “*Principios relativos al tratamiento”* del RGPD, el cual dispone: *“2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»). “*

Directamente relacionado con el principio de responsabilidad proactiva previsto en el artículo 5.2. del RGPD se encuentra la “*Responsabilidad del responsable del tratamiento*”, del artículo 24 del RGPD, el cual reza:

“1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos. (…)"

En consonancia con estas previsiones el considerando 74 del RGPD dispone: "*Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas."*

Igualmente, relacionado con el principio de responsabilidad proactiva se encuentra el principio de "*Protección de datos desde el diseño y por defecto*", recogido en el artículo 25 del RGPD, el cual establece:

"1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo".

En consonancia con estas previsiones, el considerando 78 del RGPD dispone:

"La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos

personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos".

En concreto, a la luz del RGPD considerando 78, el principio de protección de datos desde el diseño es la clave que seguir por el responsable del tratamiento para demostrar el cumplimiento con el RGPD, ya que «*el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto».*

A lo largo del procedimiento sancionador ha quedado acreditado que el sistema de permisos de acceso a los datos de los repartidores, instaurado por GLOVOAPP, no cumplía en un primer momento con estos principios y obligaciones que establece el RGPD, toda vez que la empresa no realizó un análisis previo al tratamiento en el que se analizaran debidamente las posibles implicaciones para los derechos libertades de los repartidores lo que hubiera evitado la implantación de un modelo de gestión de permisos de acceso que no garantizaba el principio de minimización. Más bien al contrario, GLOVOAPP no adoptó una postura proactiva sino más bien una actitud reactiva, modificando la gestión de los permisos de acceso a los datos personales de los repartidores como si se tratara de "parches" informáticos, solucionando los problemas a medida que se los iban encontrando conforme cambiaba la estructura de la organización, tal y como GLOVOAPP ha expuesto en sus alegaciones al acuerdo de inicio del presente procedimiento sancionador.

La libertad de empresa consagrada en el artículo 38 de la Constitución Española no es un derecho absoluto, sino que debe conjugarse con el resto de los derechos que el ordenamiento jurídico reconoce.

En este sentido, cabe traer a colación la sentencia 292/2000, de 30 de noviembre del Tribunal Constitucional, que configura el derecho a la protección de datos como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o qué datos puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Así, de acuerdo con los Fundamentos jurídicos 4, 5, 6 y 7 de la sentencia del alto tribunal:

> *"4. Sin necesidad de exponer con detalle las amplias posibilidades que la informática ofrece tanto para recoger como para comunicar datos personales ni los indudables riesgos que ello puede entrañar, dado que una persona puede ignorar no sólo cuáles son los datos que le conciernen que se hallan recogidos en un fichero sino también si han sido trasladados a otro y con qué finalidad, es*

suficiente indicar ambos extremos para comprender que el derecho fundamental a la intimidad (art. 18.1 CE) no aporte por sí sólo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico.
Ahora bien, con la inclusión del vigente art. 18.4 CE el constituyente puso de relieve que era consciente de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona. Esto es, incorporando un instituto de garantía "como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona", pero que es también, "en sí mismo, un derecho o libertad fundamental" (STC 254/1993, de 20 de julio, FJ 6). Preocupación y finalidad del constituyente que se evidencia, de un lado, si se tiene en cuenta que desde el anteproyecto del texto constitucional ya se incluía un apartado similar al vigente art. 18.4 CE y que éste fue luego ampliado al aceptarse una enmienda para que se incluyera su inciso final. Y más claramente, de otro lado, porque si en el debate en el Senado se suscitaron algunas dudas sobre la necesidad de este apartado del precepto dado el reconocimiento de los derechos a la intimidad y al honor en el apartado inicial, sin embargo, fueron disipadas al ponerse de relieve que estos derechos, en atención a su contenido, no ofrecían garantías suficientes frente a las amenazas que el uso de la informática podía entrañar para la protección de la vida privada. De manera que el constituyente quiso garantizar mediante el actual art. 18.4 CE no sólo un ámbito de protección específico sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del precepto.
5. (…)
Pues bien, en estas decisiones el Tribunal ya ha declarado que el art. 18.4 CE contiene, en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo "un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'", lo que se ha dado en llamar "libertad informática" (FJ 6, reiterado luego en las SSTC 143/1994, FJ 7, 11/1998, FJ 4, 94/1998, FJ 6, 202/1999, FJ 2). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4).
Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su

ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran.

6. La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, FJ 5; 144/1999, FJ 8; 98/2000, de 10 de abril, FJ 5; 115/2000, de 10 de mayo, FJ 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin.

De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre, FJ 4), como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado.

De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino

que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (SSTC 73/1982, de 2 de diciembre, FJ 5; 110/1984, de 26 de noviembre, FJ 3; 89/1987, de 3 de junio, FJ 3; 231/1988, de 2 de diciembre, FJ 3; 197/1991, de 17 de octubre, FJ 3, y en general las SSTC 134/1999, de 15 de julio, 144/1999, de 22 de julio, y 115/2000, de 10 de mayo), el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, FJ 7).

7. De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su

persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele."

Por tanto, cualquier actuación que suponga privar a la persona de aquellas facultades de disposición y control sobre sus datos personales, constituye un ataque y una vulneración de su derecho fundamental a la protección de datos. Y por ello se impone un deber especial de diligencia a la hora de llevar a cabo el uso o tratamiento de los datos personales, en lo que atañe al cumplimiento de los deberes que la legislación sobre protección de datos establece para garantizar los derechos fundamentales y las libertades públicas de las personas físicas, y especialmente su honor e intimidad personal y familiar, cuya intensidad se encuentra potenciada por la relevancia de los bienes jurídicos protegidos por aquellas normas y la profesionalidad de los responsables o encargados, máxime cuando operan con ánimo de lucro en el mercado de datos; en este sentido se ha pronunciado también la Sentencia de la Audiencia Nacional 392/2015, de 17 de noviembre (Ver su Fundamento de Derecho Tercero).

En definitiva, por la importancia del bien jurídico protegido, GLOVOAPP estaba obligada a encontrar soluciones de organización antes del inicio del tratamiento que garantizaran el principio de minimización y pusieran, por defecto, un límite a la accesibilidad de los datos, sin importar el tamaño de su organización ni el número de empleados con que contaba, dado que estos riesgos eran los mismos sin importar el número de repartidores en un momento determinado.

El sistema de permisos de acceso a los datos de los repartidores no se configuró debidamente en los momentos iniciales, de modo que por defecto estuviera limitado el acceso geográficamente.

Pretender que GLOVOAPP cumpliera con lo establecido en el RGPD de ninguna manera atenta contra la libertad de empresa reconocida en el artículo 38 de la Constitución Española. Simplemente, se trata de exigir que la empresa cumpla con la legalidad vigente. Y en el ámbito del derecho fundamental a la protección de los datos personales, es la AEPD quien ostenta la competencia para ello.

En tercer lugar, esta Agencia desea señalar que no se trata de que hubiera un acceso indiscriminado a datos personales, sino que el sistema de permisos de acceso a los datos personales de los repartidores no respetaba lo establecido en el apartado 2 del artículo 25 del RGPD en el sentido de "*garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento*". Ciertamente, quienes contaran con el permiso "EU User Access" tenían acceso a datos personales de repartidores que no eran necesarios para los fines de su tratamiento. Tanto así, que posteriormente este sistema de permisos de acceso fue reemplazado por otro, que otorga permisos de acceso diferenciando mediante regiones geográficas por países y/o ciudades.

Tal y como se indicó anteriormente, la responsabilidad proactiva implica la implantación de un modelo de cumplimiento y de gestión del RGPD que determina el cumplimiento generalizado de las obligaciones en materia de protección de datos. Comprende el establecimiento, mantenimiento, actualización y control de las políticas de protección de datos en una organización -entendidas como el conjunto de

directrices que rigen la actuación de una organización, prácticas, procedimientos y herramientas-, desde la privacidad desde el diseño y por defecto, que garanticen el cumplimiento del RGPD, que eviten la materialización de los riesgos y que le permita demostrar su cumplimiento.

Pivota sobre la gestión del riesgo. Tal y como se establece en el Informe 0064/2020 del Gabinete Jurídico de la AEPD se muestra la metamorfosis de un sistema que ha pasado de ser reactivo a convertirse en proactivo, puesto que "*en el momento actual, hay que tener en cuenta que el RGPD ha supuesto un cambio de paradigma al abordar la regulación del derecho a la protección de datos personales, que pasa a fundamentarse en el principio de «accountability» o «responsabilidad proactiva» tal y como ha señalado reiteradamente la AEPD (Informe 17/2019, entre otros muchos) y se recoge en la Exposición de motivos de la LOPDGDD: "la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan".*

Requiere de una actitud consciente, comprometida, activa y diligente. La consciencia supone el conocimiento de su organización por parte del responsable del tratamiento y de cómo se ve afectada por la protección de datos y de los riesgos inherentes a los tratamientos de datos personales; el compromiso involucra la voluntad de cumplir y el hacerse verdaderamente responsable de la implantación de las políticas de protección de datos en la organización; la actitud activa está relacionada con la proactividad, la eficacia, la eficiencia y la operatividad; y la diligencia es el cuidado, el celo y la dedicación puesta en el cumplimiento.

GLOVO debió tener en cuenta en el proceso de diseño las medidas aplicables a su sistema de accesos orientadas al cumplimiento del principio de minimización, lo que no consta que haya hecho, circunstancia que supone una infracción del art. 25.1 del RGPD

Por otro lado, para el cumplimiento del principio de protección de datos por defecto, el responsable del tratamiento no debe recoger más datos de los que sean necesarios, ni realizar un tratamiento de los datos recogidos más amplio de lo necesario para sus fines, ni conservar los datos durante más tiempo del necesario. El requisito básico es que la protección de datos esté integrada en el tratamiento por defecto, como se recoge en las Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto.

Sentado lo anterior, puede afirmarse que, de la instrucción del procedimiento, se constató, entre otros, la falta de medidas adecuadas para garantizar que, por defecto, sólo se iban a tratar los datos necesarios para la finalidad pretendida, lo que constituye una infracción del artículo 25.2 del RGPD

Tampoco se estableció un mecanismo que limitara el acceso de los usuarios a los datos que no resultaban necesarios, circunstancia que incumple el art. 32 del RGPD.

En cuarto lugar, esta Agencia reconoce que GLOVOAPP contaba con diferentes perfiles de usuarios, que existía una propiedad del perfil de usuario que proporcionaba acceso, o no, a datos de los repartidores europeos, “EU User Access” y que quien no disponía de este permiso únicamente podía acceder a datos básicos del repartidor; que el “EU User Access” era una característica de perfil utilizada en la práctica en el momento de la inspección; y que no todos los perfiles podían acceder a la información de los repartidores ni modificarla.

Lo que esta Agencia cuestiona, precisamente, no es la falta de perfiles sino la falta de unos perfiles de usuario que permitieran únicamente acceso a los datos de los repartidores de la zona geográfica adecuada. No se trata de que hubiera perfiles que no permitieran el acceso a los datos de los repartidores sino de que los que permitían el acceso posibilitaban el acceso a más datos de los necesarios. Es decir, se trata, en el presente caso, de que, dentro de los perfiles que debían tener acceso a los datos de los repartidores, no había perfiles diferenciados por regiones, países, ciudades, u otro parámetro similar. Funcionalidad que sí fue incorporada con posterioridad.

En quinto lugar, el RGPD no realiza distinciones en cuanto a las obligaciones de los responsables de tratamiento en función del tamaño o crecimiento que experimente la empresa, ni el esquema de desarrollo empresarial que utilice, ni según la forma en que decida organizarse para llevar a cabo sus actividades.

El RGPD se limita a señalar que los responsables de tratamiento deben cumplir con las obligaciones en él establecidas. Respecto al artículo 25 del RGPD, el responsable del tratamiento debe aplicar, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados. Y debe aplicar las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Y respecto del artículo 32 del RGPD, el responsable del tratamiento debe aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

Lo que sí señala el RGPD es que, en ambos casos, se tendrá en cuenta una serie de factores para identificar las medidas en cuestión, como el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

Pero el hecho de que fuera una empresa en expansión, ni que utilizara una metodología ágil, ni siquiera que decidiera centralizar la atención a sus clientes o repartidores en un sitio determinado resulta en una situación que pudiera exceptuar a GLOVOAPP de cumplir con lo establecido en la normativa.

Precisamente, ha debido prever antes de iniciar el tratamiento en cuestión qué medidas aplicaría. Y una vez iniciada su actividad, a medida que la empresa iba creciendo y operando en más países y ciudades, debió también revisar si las medidas técnicas y organizativas eran las adecuadas. Y GLOVOAPP debió arbitrar los medios

necesarios para que el personal que debía acceder a los datos de los repartidores sólo pudiera acceder a los datos necesarios para desempeñar su trabajo, ni más ni menos.

Aun en el supuesto de que se tratara de una actividad externalizada realizada desde una única sede, la mera organización del trabajo indica que cada trabajador no estaría en posición de gestionar el volumen total de peticiones, sino que la tarea estaría repartida, más teniendo en cuenta que se trata de países que ni siquiera comparten un idioma común. Por tanto, había personal que tenía acceso a datos de los repartidores de países de los que no era necesario que lo tuvieran, dado que no tramitarían peticiones de éstos.

Y ha quedado acreditado en el expediente que los permisos proporcionados al personal adscrito al departamento de atención al cliente o atención al repartidor tenía acceso a los datos de todos los repartidores de la Unión Europea, sin estar limitados de ninguna manera, ni por países, ni ciudades, ni regiones, ni nada.

En sexto lugar, esta Agencia desea señalar que el citado DOCUMENTO 30 que fue aportado junto con el escrito de alegaciones al acuerdo de inicio del PS/00020/2021 no es otro que una “Checklist previa a la evaluación de impacto” (tal como reza su descripción), en el que GLOVOAPP se limita a “Comprobar si un tratamiento reúne las características para realizar una evaluación de impacto en materia de protección de datos” (tal como reza en su apartado “Tratamiento”). En cuanto a su contenido, se trata de un documento en el que se revisa únicamente si se realiza:

- ***(…)***

En ninguno de estos documentos se hace un análisis de los riesgos de los datos personales de los repartidores ni se hace referencia a medida alguna, ni planificada ni implementada desde el diseño que prevenga el incumplimiento del principio de minimización ni garantice que, por defecto, no se traten datos de los repartidores que no sean necesarios, como exige el artículo 25. Tampoco constan medidas para garantizar la seguridad de estos datos, tal y como obliga el artículo 32 del RGPD.

El artículo 25 del RGPD establece que: “*Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados. (…*)”

Y el artículo 32 del RGPD establece que: “*Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo (…)”*

En el presente caso en ninguno de los documentos aportados la parte recurrente hace referencia a los posibles riesgos a los que podrían estar expuestos los datos de los repartidores ni tampoco se hace referencia a las medidas técnicas y organizativas apropiadas para *aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados (artículo 25 RGPD)* ni hace referencia a las medidas técnicas y organizativas apropiadas *para garantizar un nivel de seguridad adecuado al riesgo* (artículo 32 RGPD).

Por tanto, no cabe entender que de estos documentos se desprenda que GLOVOAPP hubiera analizado debidamente, al determinar los medios del tratamiento ni durante la realización del mismo, el *estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas,* a fin de adoptar las correspondientes medidas.

En séptimo lugar, las *Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto Versión 2.0*, adoptadas por el Comité Europeo de Protección de Datos el 20 de octubre de 2020 disponen que:

"(…) La protección de datos desde el diseño debe llevarse a cabo «en el momento de determinar los medios de tratamiento».
(…)
El «momento de determinar los medios de tratamiento» hace referencia al período de tiempo en que el responsable está decidiendo de qué forma llevará a cabo el tratamiento y cómo se producirá este, así como los mecanismos que se utilizarán para llevar a cabo dicho tratamiento. En el proceso de adopción de tales decisiones, el responsable del tratamiento debe evaluar las medidas y garantías adecuadas para aplicar de forma efectiva los principios y derechos de los interesados en el tratamiento, y tener en cuenta elementos como los riesgos, el estado de la técnica y el coste de aplicación, así como la naturaleza, el ámbito, el contexto y los fines. Esto incluye el momento de la adquisición y la implementación del software y hardware y los servicios de tratamiento de datos.
(…)
Una vez iniciado el tratamiento, el responsable tiene la obligación permanente de mantener la PDDD, es decir, aplicar los principios de forma efectiva y continuada a fin de proteger los derechos, mantenerse al día del estado de la técnica, reevaluar el nivel de riesgo, etcétera. La naturaleza, el ámbito y el contexto de las operaciones de tratamiento, así como el riesgo, pueden cambiar durante el curso del tratamiento, lo que significa que el responsable deberá reevaluar sus operaciones de tratamiento revisando y valorando periódicamente la efectividad de las medidas y garantías que haya decidido adoptar.

La obligación de mantener, revisar y actualizar la operación de tratamiento, según sea necesario, también se aplica a los sistemas ya existentes. Esto significa que los sistemas heredados que se hayan diseñado antes de la entrada en vigor del RGPD deben someterse a revisión y mantenimiento para asegurar que se aplican medidas y garantías que apliquen los principios y derechos de los interesados de forma efectiva, como se explica en estas Directrices.

(…)
El responsable del tratamiento debe determinar previamente con qué fines especificados, explícitos y legítimos se recogen y se tratan los datos personales. Las medidas deben ser adecuadas para garantizar, por defecto, que solo se traten los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. (…)
Las mismas consideraciones son aplicables a las medidas organizativas de apoyo a las operaciones de tratamiento. Deben estar concebidas para tratar, desde el principio, únicamente la cantidad de datos personales mínima necesaria para las operaciones específicas. Esto debe tenerse especialmente en cuenta a la hora de asignar el acceso a los datos a personas con diferentes funciones y diferentes necesidades de acceso.

Las «medidas técnicas y organizativas» adecuadas en el contexto de la protección de datos por defecto se entienden pues de la manera ya explicada en el apartado 2.1.1, pero específicamente con respecto a la aplicación del principio de minimización de datos. (…)"

En especial, las citadas Directrices dicen que:

"(…) En el considerando 78 se afirma que una de las medidas de PDDD podría consistir en permitir al responsable del tratamiento «crear y mejorar elementos de seguridad». Junto con otras medidas de PDDD, el considerando 78 apunta que los responsables del tratamiento tienen la responsabilidad de evaluar de forma continua si están utilizando medios apropiados de tratamiento en todo momento y si las medidas elegidas neutralizan verdaderamente las vulnerabilidades existentes. Además, los responsables del tratamiento deben llevar a cabo revisiones periódicas de las medidas de seguridad de la información que rodean y protegen los datos personales, así como el procedimiento para gestionar vulneraciones.

Elementos esenciales desde el diseño y por defecto con respecto a la integridad y la confidencialidad pueden ser los siguientes:
(…)
• Análisis de riesgos: Se evaluarán los riesgos contra la seguridad de los datos personales teniendo en cuenta cómo afectan a los derechos de las personas y se neutralizarán los riesgos identificados. Para su uso en la evaluación de riesgos, se desarrollará y mantendrá un «modelo de amenazas» exhaustivo, sistemático y realista y un análisis de la superficie de ataque del software diseñado para reducir los vectores de ataque y las oportunidades de aprovechar puntos débiles y vulnerabilidades.

• Seguridad desde el diseño: Se considerarán los requisitos de seguridad lo antes que sea posible en el diseño y desarrollo del sistema y se integrarán y realizarán los ensayos pertinentes de forma continuada.

• Mantenimiento: Se realizarán revisiones y ensayos periódicos del software, hardware, sistemas y servicios, etcétera, para detectar vulnerabilidades de los sistemas de apoyo al tratamiento.

• *Gestión del control de acceso: Solo el personal autorizado que lo necesite deberá tener acceso a los datos personales necesarios para sus tareas de tratamiento, y el responsable deberá diferenciar los privilegios de acceso del personal autorizado.*

o Limitación de acceso (agentes): Se configurará el tratamiento de datos de manera que se minimice el número de personas que necesiten acceder a datos personales para desempeñar sus funciones, y se limitará el acceso en consecuencia.

o Limitación de acceso (contenido): En el contexto de cada operación de tratamiento, se limitará el acceso exclusivamente a aquellos atributos de cada conjunto de datos que sean necesarios para realizar esa operación. Además, se limitará el acceso a los datos que pertenezcan a aquellos interesados que estén incluidos en el ámbito de competencia del empleado respectivo.

o Segregación de acceso: Se configurará el tratamiento de datos de manera que ninguna persona necesite acceder a todos los datos de un interesado, y mucho menos a todos los datos personales de una determinada categoría de interesados. (…)"

En el presente caso, la parte recurrente inició su actividad en el año 2015. En el supuesto documento de análisis de riesgos que realizó en el año 2017, que se aporta como DOCUMENTO 30 junto con el escrito de alegaciones al acuerdo de inicio del PS/00020/2021, el cual lleva como descripción "Checklist previa a la evaluación de impacto", ha quedado acreditado que simplemente se verificó si era necesaria o no realizar una evaluación de impacto de protección de datos personales. Y en el supuesto documento de análisis de riesgos que la parte recurrente realizó en el año 2019, obtenido durante la inspección presencial que realizó esta Agencia, ha quedado acreditado que se limita a analizar si (a su entender) es necesaria una evaluación de impacto en base a lo dispuesto por el artículo 35 del RGPD y si dicha empresa realiza alguna de las actividades establecidas en la lista que esta Agencia tenía publicada en su página web.

Pero en ninguno de ambos casos ha quedado acreditado que la parte recurrente hubiera evaluado al determinar los medios de tratamiento "*las medidas y garantías adecuadas para aplicar de forma efectiva los principios y derechos de los interesados en el tratamiento"* ni que una vez iniciado el tratamiento hubiera reevaluado *"sus operaciones de tratamiento revisando y valorando periódicamente la efectividad de las medidas y garantías que haya decidido adoptar".*

Es más, en el caso concreto, la parte recurrente había iniciado su actividad antes de la entrada en vigor del RGPD por lo que le resulta de especial aplicación aquello de que *"significa que los sistemas heredados que se hayan diseñado antes de la entrada en vigor del RGPD deben someterse a revisión y mantenimiento para asegurar que se aplican medidas y garantías que apliquen los principios y derechos de los interesados de forma efectiva, como se explica en estas Directrices".*

El hecho de que recién a mediados de 2020 se cambiara el sistema de permisos del personal que podía acceder a los datos de los repartidores de toda Europa implica que durante años el sistema de permisos no fue sometido a revisión ni se analizaron los posibles riesgos para los derechos y libertades de los interesados ni se adoptaron las medidas necesarias para garantizar que se cumplía con los principios de tratamiento que establece el RGPD.

Es más, en cuanto a que *"Las medidas deben ser adecuadas para garantizar, por defecto, que solo se traten los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento"* las citadas Directrices realizan hincapié en que *"Esto debe tenerse especialmente en cuenta a la hora de asignar el acceso a los datos a personas con diferentes funciones y diferentes necesidades de acceso".* Y se insiste en la *"responsabilidad de evaluar de forma continua si están utilizando medios apropiados de tratamiento en todo momento y si las medidas elegidas neutralizan verdaderamente las vulnerabilidades existentes",* lo cual no se ha realizado en el presente caso.

No se ha realizado un análisis de riesgos en condiciones, en el que se desarrolle *"un «modelo de amenazas» exhaustivo, sistemático y realista y un análisis de la superficie de ataque del software diseñado para reducir los vectores de ataque y las oportunidades de aprovechar puntos débiles y vulnerabilidades".*

Ni tampoco se ha realizado correctamente la gestión del control de acceso, en especial a lo relativo a la segregación de acceso, dado que la parte recurrente misma reconoce que todo el personal de atención al cliente o repartidor podía acceder a todos los datos personales de los repartidores de la Unión Europea.

Sentado lo anterior, puede afirmarse que, de la instrucción del procedimiento, se constató, entre otros, la falta de un sistema de permisos de acceso a los datos personales de los repartidores que tuviera en cuenta desde un inicio los riesgos y libertades para sus derechos, lo que denota una actitud reactiva y no proactiva enfocada desde el diseño. Y en este sentido es que esta Agencia considera que la parte recurrente no ha sido todo lo diligente que debiera haber sido a la hora de configurar el sistema de permisos del personal encargado de la atención al cliente o al repartidor. El hecho de que la organización empresarial de la compañía hubiera variado en el tiempo no obsta a que en todo momento la empresa debió prever las medidas adecuadas para garantizar el cumplimiento del RGPD y proteger los derechos y libertades de los repartidores.

A mayor abundamiento, el considerando 78 del RGPD dispone:

"La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se

aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos".

En concreto, a la luz del considerando 78 del RGPD, el principio de protección de datos desde el diseño es la clave a seguir por el responsable del tratamiento para demostrar el cumplimiento con el RGPD, ya que *«el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto».*

El principio de privacidad desde el diseño es una muestra del paso de la reactividad a la proactividad y manifestación directa del enfoque de riesgos que impone el RGPD. Parte de la responsabilidad proactiva, impone que, desde los estadios más iniciales de planificación de un tratamiento debe de ser considerado este principio: el responsable del tratamiento desde el momento en que se diseña y planifica un eventual tratamiento de datos personales deberá determinar todos los elementos que conforman el tratamiento, a los efectos de aplicar de forma efectiva los principios de protección de datos, integrando las garantías necesarias en el tratamiento con la finalidad última de, cumpliendo con las previsiones del RGPD, proteger los derechos de los interesados.

Así, y respecto de los riesgos que pueden estar presentes en el tratamiento, el responsable del tratamiento llevará a cabo un ejercicio de análisis y detección de los riesgos durante todo el ciclo de tratamiento de los datos, con la finalidad primera y última de proteger los derechos y libertades de los interesados, y no sólo cuando efectivamente se produce el tratamiento. Así se expresa en las citadas Directrices 4/2019 cuando afirman que:

"*Tomar en consideración la PDDD desde un principio es crucial para la correcta aplicación de los principios y para la protección de los derechos de los interesados. Además, desde el punto de vista de la rentabilidad, también interesa a los responsables del tratamiento tomar la PDDD en consideración cuanto antes, ya que más tarde podría resultar difícil y costoso introducir cambios en planes ya formulados y operaciones de tratamiento ya diseñadas".*

Para ello debe recurrir al diseñar el tratamiento a los principios recogidos en el artículo 5 del RGPD, que servirán para aquilatar el efectivo cumplimiento del RGPD. Así, las citadas Directrices 4/2019 disponen que *"Para hacer efectiva la PDDD, los responsables del tratamiento han de aplicar los principios de transparencia, licitud, lealtad, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad, y responsabilidad proactiva. Estos principios están recogidos en el artículo 5 y el considerando 39 del RGPD".*

La Guía de Privacidad desde el Diseño de la AEPD afirma que *"La privacidad desde el diseño (en adelante, PbD) implica utilizar un enfoque orientado a la gestión del riesgo y de responsabilidad proactiva para establecer estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida del objeto (ya sea este un sistema, un producto hardware o software, un servicio o un proceso). Por ciclo de vida del objeto se entiende todas las etapas por las que atraviesa este, desde su concepción*

hasta su retirada, pasando por las fases de desarrollo, puesta en producción, operación, mantenimiento y retirada".

La Guía dispone que *"La privacidad debe formar parte integral e indisoluble de los sistemas, aplicaciones, productos y servicios, así como de las prácticas de negocio y procesos de la organización. No es una capa adicional o módulo que se añade a algo preexistente, sino que debe estar integrada en el conjunto de requisitos no funcionales desde el mismo momento en el que se concibe y diseña (…) La privacidad nace en el diseño, antes de que el sistema esté en funcionamiento y debe garantizarse a lo largo de todo el ciclo de vida de los datos".*

Por ello, la privacidad desde el diseño, obligación del responsable del tratamiento que nace antes de que el sistema esté en funcionamiento, no son parches que se van asentando sobre un sistema construido de espaldas al RGPD. Ligado a la edificación de una verdadera cultura de protección de datos en la organización, implica también por mor de la responsabilidad proactiva la capacidad de documentar todas las decisiones que se adopten con un enfoque "privacy design thinking", demostrando el cumplimiento del RGPD también en este aspecto.

El enfoque de riesgos hace referencia directa e inmediata a un sistema preventivo tendente a visualizar, respecto de un tratamiento de datos personales, los riesgos en los derechos y libertades de las personas físicas. Ha de excluirse, por tanto, del enfoque de riesgos de protección de datos otra serie de riesgos a los que puede encontrarse sometida la organización y que afecten a su ámbito de negocio.

En relación con los riesgos en los derechos y libertades de las personas físicas, han de identificarse los riesgos, evaluar su impacto y valorar la probabilidad de que aquellos se materialicen. Se protegen pues, no los datos, sino a las personas que están detrás de ellos.

En el presente caso, en los supuestos análisis de riesgos de GLOVOAPP, de 2017 y 2019, se observa que ambos tienen por finalidad simplemente concluir que no era necesaria realizar una evaluación de impacto en materia de protección de datos, pero no garantizar el Derecho Fundamental a la Protección de Datos Personales de los repartidores, no se protegen sus derechos y libertades, que es la finalidad última que persigue el RGPD a través de la protección de datos desde el diseño. No se trata, por lo tanto, de un documento concebido para el cumplimiento del principio de responsabilidad proactiva (artículo 5.2 RGPD), ya que para ello debería haberse partido de un adecuado análisis de riesgos que llevara a la adopción de medidas para la protección de los derechos y libertades, a partir siempre del diseño del tratamiento. Desde esta óptica, en la ya mencionada Guía de Privacidad desde el diseño de la AEPD se establecen diversas orientaciones, que no se cumplen en el presente caso:

"Cualquier sistema, proceso o infraestructura que vaya a utilizar datos personales debe ser concebida y diseñada desde cero identificando, a priori, los posibles riesgos a los derechos y libertades de los interesados y minimizarlos para que no lleguen a concretarse en daños. Una política de PbD se caracteriza por la adopción de medidas proactivas que se anticipan a las amenazas, identificando las debilidades de los sistemas para neutralizar o minimizar los riesgos en lugar de aplicar medidas correctivas para resolver los incidentes de seguridad una vez sucedidos. Es decir, la PbD huye de

la "política de subsanar" y se adelanta a la materialización del evento de riesgo".

La privacidad como configuración predeterminada:

"La PbD persigue proporcionar al usuario el máximo nivel de privacidad dado el estado del arte y, en particular, que los datos personales estén automáticamente protegidos en cualquier sistema, aplicación, producto o servicio. La configuración por defecto deberá quedar establecida desde el diseño a aquel nivel que resulte lo más respetuoso posible en términos de privacidad. En el caso de que el sujeto no tome ninguna acción de configuración, su privacidad debe estar garantizada y mantenerse intacta, pues está integrada en el sistema y configurada por defecto.

Privacidad incorporada en la fase de diseño:

"*La privacidad debe formar parte integral e indisoluble de los sistemas, aplicaciones, productos y servicios, así como de las prácticas de negocio y procesos de la organización. No es una capa adicional o módulo que se añade a algo preexistente, sino que debe estar integrada en el conjunto de requisitos no funcionales desde el mismo momento en el que se concibe y diseña. Para garantizar que la privacidad se tiene en cuenta desde las primeras etapas del diseño se debe:*
• Considerar como un requisito necesario en el ciclo de vida de sistemas y servicios, así como en el diseño de los procesos de la organización.
• Ejecutar un análisis de los riesgos para los derechos y libertades de las personas y, en su caso, evaluaciones de impacto relativas a la protección de datos, como parte integral del diseño de cualquier nueva iniciativa de tratamiento.
• Documentar todas las decisiones que se adopten en el seno de la organización con un enfoque "privacy design thinking".

Respeto por la privacidad de los usuarios, manteniendo un enfoque centrado en el usuario:

"Sin obviar los intereses legítimos que persigue la organización con el tratamiento de datos que realiza, el fin último debe ser garantizar los derechos y libertades de los usuarios cuyos datos son objeto de tratamiento, por lo que cualquier medida adoptada debe ir encaminada a garantizar su privacidad. Ello supone diseñar procesos, aplicaciones, productos y servicios "con el usuario en mente", anticipándose a sus necesidades. El usuario debe tener un papel activo en la gestión de sus propios datos y en el control de la gestión que otros hagan con ellos. Su inacción no debe suponer un menoscabo a la privacidad, retomando uno de los principios ya mencionados y que propugna una configuración de privacidad por defecto que ofrezca el máximo nivel de protección".

Así, el sistema de permisos de acceso a los datos personales de los repartidores requiere, en materia de protección de datos, de un correcto análisis de los riesgos en los derechos y libertades de los repartidores, de una adecuada planificación, del establecimiento de medidas de seguridad evitativas de los riesgos, de un mantenimiento, actualización y control de aquellas desde la revisión continua de los riesgos, incluyendo la demostración del cumplimiento (observancia del principio de responsabilidad proactiva), especialmente, en el presente caso que nos atañe, en relación con las medidas de seguridad apropiadas. Y ello con el objeto de que se garantice el Derecho Fundamen-

tal a la Protección de Datos de los repartidores, que incluye la efectiva protección de los datos personales por los interesados, así como garantizar la seguridad de los datos personales de los clientes de manera efectiva y en particular, que estos datos personales no pudieran ser accesibles por personal para el cual este acceso no fuera necesario. El cumplimiento de esta obligación impuesta por el RGPD al responsable del tratamiento se logra a través de la privacidad desde el diseño.

Así, examinado el sistema de permisos del personal de atención al cliente o repartidor denominado “UE User Access”, se ha constatado que el mismo no cumplía con las previsiones del RGPD y no estaba enfocado en los riesgos para los derechos y libertades de los clientes, lo que muestra que no se ha cumplido con la obligación dispuesta en el artículo 25 del RGPD en relación con el diseño y la integración de la protección de datos en el mencionado sistema de permisos.

Por último, respecto al citado DOCUMENTO 1 que se acompaña al presente recurso de reposición, este viene fechado 23 de septiembre de 2020, es decir, meses después de que el sistema de permisos de la parte recurrente fuera modificado. Además, la propia parte recurrente indica que podría haberlo aportado antes, por lo que en virtud del artículo 118.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas no será tenido en cuenta para la resolución del presente recurso.

SEGUNDO-. NULIDAD DE LA RESOLUCIÓN SANCIONADORA POR AUSENCIA DE LOS ELEMENTOS NECESARIOS PARA QUE SE CONSIDERE QUE EXISTE INFRACCIÓN.

2.1 Ausencia de los elementos subjetivos de la infracción. Nulidad de Sanción.

Alega la parte recurrente que no concurren los elementos fundamentales y requisitos necesarios para poder imponer una sanción en el caso objeto de controversia.

E insiste en que los principios que rigen la potestad sancionadora de la Administración deben ser, con carácter general, los propios del Derecho Administrativo Sancionador y en particular, “los principios de legalidad, tipicidad, responsabilidad, proporcionalidad y no concurrencia”.

Alega que la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, la “LRJSP”) establece que la infracción administrativa viene constituida por la acción, entendida en sentido amplio de toda actuación -u omisión- de las personas encaminadas a la producción de un resultado y que el propio Legislador ha tipificado como infracción.

De acuerdo con lo anterior, para poder estar ante una infracción en materia de protección de datos personales debe de haberse producido una acción u omisión dolosa o culposa con cualquier grado de negligencia.

Y que esto quiere decir que al sujeto responsable se le podía, cuando menos, haber exigido una conducta distinta.

Alega que se pueden definir los elementos subjetivos del tipo como los diferentes grados de voluntariedad o, cuando menos, inobservancia de la diligencia debida; siendo el dolo el claro exponente de la voluntariedad en la comisión de la acción típica y la simple negligencia la conducta carente del cuidado necesario en el cumplimiento de las obligaciones.

De esta forma, corresponde al órgano competente examinar si la conducta objeto de análisis es dolosa o culposa, ya que dicha valoración es imprescindible para poder imponer una sanción pues se trata de elementos constitutivos de la infracción administrativa.

En su apoyo, la parte recurrente cita los párrafos a su juicio más representativos de la Sentencia de 13 de octubre de 2005 de la Audiencia Nacional.

Alega que es precisamente el análisis de la culpabilidad lo que diferencia a un sistema de responsabilidad objetiva, en el que se sanciona exclusivamente atendiendo al resultado, de uno basado en el principio de culpabilidad.

Y que la Resolución Sancionadora prescinde de uno de los elementos esenciales a la hora de poder imponer una sanción, como es el examen de la culpabilidad.

Por tanto, debe tenerse en cuenta que la Administración debía llevar a cabo este análisis y por tanto, no pudiendo apreciarse de ningún modo ánimo de infringir por parte de Glovo y habiéndose prescindido de la valoración de dicho ánimo como elemento esencial de la infracción administrativa, la imposición de sanción estaría viciada de nulidad.

Alega la parte recurrente que antes una posible sanción de 550.000 euros, se debería haber realizado un análisis de la conducta bastante más diligente, por lo que debería declararse nula de pleno derecho por falta de motivación la sanción aplicada a Glovo.

Al respecto, esta Agencia desea señalar que en la Resolución Sancionadora se ha llevado a cabo un detallado examen de la culpabilidad, a través de al menos 9 páginas, las dedicadas a contestar los puntos 3.4, 5.1 y 5.3 de las alegaciones aducidas al acuerdo de inicio del procedimiento sancionador, en las que se concluye que la actuación de la parte recurrente ha sido negligente, razón por la que se le han imputado las infracciones de referencia.

Por lo demás, sólo cabe reiterar lo ya expuesto en la citada Resolución Sancionadora objeto del presente recurso.

En este sentido, esta Agencia considera que la parte recurrente no actuó diligentemente.

Negar la concurrencia de una actuación negligente por parte de la parte recurrente equivaldría a reconocer que su conducta -por acción u omisión- ha sido diligente. Obviamente, no se comparte esta perspectiva de los hechos, puesto que ha quedado acreditada la falta de diligencia debida.

Esta Agencia se reitera en que a lo largo del presente procedimiento ha quedado acreditado que el sistema de permisos de acceso a los datos de los repartidores, instaurado por la parte recurrente, no cumplía en un primer momento con estos principios y obligaciones que establece el RGPD, toda vez que la empresa no realizó un análisis previo al tratamiento en el que se analizaran debidamente las posibles implicaciones para los derechos y libertades de los interesados y se determinaran en base al mismo las medidas adecuadas al sistema de gestión de permisos de acceso Más bien al contrario, la parte recurrente no adoptó una postura proactiva sino más bien una actitud reactiva, modificando la gestión de los permisos de acceso a los datos personales de los repartidores como si se tratara de "parches" informáticos, solucionando los problemas a medida que se los iban encontrando conforme cambiaba la estructura de la organización, tal y como la parte recurrente ha expuesto en sus alegaciones durante el procedimiento sancionador objeto del presente recurso.

Por la importancia del bien jurídico protegido, la parte recurrente estaba obligada a encontrar soluciones de organización que no supusieran un mayor riesgo para los derechos y libertades de sus repartidores y que garantizaran la seguridad de los datos, sin importar el tamaño de su organización ni el número de empleados con que contaba, dado que estos riesgos eran los que debían tenerse en cuenta sin importar el número de repartidores en un momento determinado.

El sistema de permisos de acceso a los datos de los repartidores no se configuró en los momentos iniciales teniendo en cuenta los posibles riesgos para los derechos y libertades de sus repartidores ni se configuró de modo que, por defecto, no resultaran accesibles los datos de los repartidores si no era necesario para la finalidad. La parte recurrente debió asegurarse de que, por defecto, el acceso a los datos de los repartidores estuviera limitado al ámbito geográfico necesario, en cumplimiento del artículo 25.2 del RGPD.

Sentado lo anterior, puede afirmarse que, de la instrucción del procedimiento, se constató también, entre otros, la falta de un mecanismo de permisos de acceso a los datos personales de los repartidores que impidiera el acceso de los usuarios a datos que no eran necesarios y que garantizara la seguridad de los datos, como exige el art. 32 del RGPD.

Igualmente, el hecho de que la parte recurrente hubiera implementado posteriormente modificaciones en las medidas técnicas u organizativas existentes, corrobora que aquellas otras no proporcionaban la seguridad adecuada.

Respecto a la infracción del artículo 13 del RGPD, esta Agencia considera que la parte recurrente debió ser diligente a la hora de realizar un análisis previo y concomitante al tratamiento, a fin de establecer la información que debía facilitar a los repartidores sobre el sistema "excellence score".

De haber obrado diligentemente, la parte recurrente habría realizado las comprobaciones pertinentes y habría comprobado que se estaban realizando decisiones individuales automatizadas de las del artículo 22 del RGPD y que debía, por tanto, informarse a los repartidores de su existencia, además de proporcionar toda la información exigida por el artículo 13 del RGPD.

2.2. Falta de prueba que desvirtúe la presunción de inocencia de Glovo. Nulidad de sanción

Alega la parte recurrente que para proceder a la imposición de cualquier sanción administrativa es requisito previo e inexcusable la existencia de una conducta constitutiva de infracción administrativa.

Y que, la Administración no puede sancionar sin probar suficientemente la culpabilidad del sujeto sancionado, es decir, la existencia de mala fe en su conducta. En consecuencia, queda claro que corresponde a la Administración la carga de la prueba de la culpabilidad del sujeto, la cual deberá quedar acreditada por cualquiera de los medios admitidos en derecho.

Pero que, en el presente caso, no consta a Glovo que exista absolutamente ningún elemento probatorio que permita considerar destruida la presunción de inocencia que, dentro del ámbito administrativo-sancionador, es plenamente aplicable a las relaciones entre la Administración y los administrados, tal y como han reconocido innumerables resoluciones jurisdiccionales en todos los ámbitos jerárquicos y territoriales.

Y cita, por ejemplo, la Sentencia del Tribunal Superior de Justicia de 10 de junio de 1994 y la Sentencia del Tribunal Supremo de 26 de diciembre de 1983 (RJ 1983\6418).

Alega la parte recurrente que a la Resolución Sancionadora de la AEPD se le debe exigir algo más que la simple mención a los preceptos legales. Y que, en el presente caso, la Resolución Sancionadora se limita otra vez a repasar los antecedentes del expediente pero no se puede de ningún modo afirmar que nos encontramos ante una infracción intencionada de la normativa de protección de datos por parte de Glovo.

El objetivo principal del procedimiento sancionador debe ser, en opinión de Glovo, precisamente no quedarse en lo ya señalado en el procedimiento, sino tratar de romper la presunción de inocencia que asiste a todo obligado buscando el elemento intencional en su actuación, el elemento subjetivo del ilícito administrativo a través de una actividad probatoria que pueda ser considerada suficiente. Sin embargo, en el presente caso, al no haber efectuado actividad probatoria alguna, no existen evidentes pruebas de cargo en dicha Resolución Sancionadora que permitan entender que existe culpabilidad en la conducta de Glovo.

Por todos los argumentos expuestos, la parte recurrente solicita que se declare la nulidad de pleno derecho del acuerdo de imposición de las sanciones impuestas a Glovo en la Resolución Sancionadora de la AEPD, al haber sido dictada con una ausencia total de elementos probatorios de la culpabilidad y, en consecuencia, con violación del derecho fundamental a la presunción de inocencia recogido en la Constitución Española.

Al respecto, esta Agencia desea reiterar lo ya expuesto en la citada Resolución Sancionadora objeto del presente recurso.

En primer lugar, esta Agencia desea señalar que existen numerosas evidencias del comportamiento de la parte recurrente, todas las cuales constan en el expediente. No

sólo se han recabado todas las evidencias recogidas durante la inspección presencial, sino también toda la información aportada por la parte recurrente mediante sus respuestas a los requerimientos de información de esta Agencia y sus alegaciones al acuerdo de inicio del procedimiento sancionador número PS/00020/2021, así como las alegaciones a la propuesta de resolución del citado procedimiento sancionador, junto con la documentación que a ellas se acompaña, así como las alegaciones al acuerdo de inicio del presente procedimiento sancionador. Todo ello según se recoge en los hechos probados de la citada Resolución Sancionadora.

En segundo lugar, esta Agencia desea insistir en que no considera que la parte recurrente hubiera infringido de forma deliberada la normativa de protección de datos, sino que se considera que no ha obrado con la debida diligencia que hubiera debido, habida cuenta del tratamiento continuo de datos personales que realizaba.

En tercer lugar, se le imputó a la parte recurrente la comisión las siguientes infracciones:

- Una infracción del artículo 13 del RGPD por no informar debidamente a los repartidores sobre la realización de decisiones individuales automatizadas (mediante la utilización del sistema “excellence score”): A lo largo del procedimiento sancionador ha quedado debidamente acreditado que la parte recurrente realizaba tales decisiones y que no informaba de ello debidamente a sus repartidores en los documentos pertinentes.

- También se le imputa la infracción de los artículos 25 y 32 del RGPD: En el presente caso, ha quedado debidamente acreditado a lo largo del procedimiento sancionador que la parte recurrente tenía implantado un sistema de permisos de acceso a los datos de los repartidores que no cumplía con las exigencias del artículo 32, toda vez que otorgaba acceso a datos que no eran necesarios para los fines otorgados. Y que tampoco actuó con diligencia por su parte a la hora de realizar un análisis adecuado previo al inicio del tratamiento sobre la información de los repartidores que debía facilitarse a los usuarios por ser necesaria para la consecución de los fines y la que debía quedar limitada por defecto.

Por todo lo expuesto, se desestima la presente alegación.

2.4. Ausencia del principio de tipicidad y presunción de inocencia. Nulidad de sanción

La parte recurrente alega la inexistencia de las conductas consideradas como infracción y por las cuales se le sanciona en vía administrativa. Y que ello debería haber llevado a la AEPD a archivar de nuevo las actuaciones sancionadoras contra Glovo puesto que, de no ser así, se incurriría en una flagrante vulneración del principio de tipicidad que se desprende de la normativa de aplicación.

Indica la parte recurrente que el ordenamiento jurídico protege a los administrados en el procedimiento sancionador exigiendo que los órganos administrativos encargados del impulso de actuaciones sancionadoras sólo consideren como infracciones aquellas conductas que encajen adecuadamente en las definiciones que explícitamente

establezcan normas con rango legal. Así, el primer apartado del artículo 129 de la LRJSP, establece lo siguiente:

"Artículo 27. Principio de tipicidad.
1. Sólo constituyen infracciones administrativas las vulneraciones del ordenamiento jurídico previstas como tales infracciones por una Ley, sin perjuicio de lo dispuesto para la Administración Local en el Título XI de la Ley 7/1985, de 2 de abril"

Alega la parte recurrente que la misma LRJSP establece que el punto de partida de toda actuación encaminada a establecer responsabilidades por la comisión de infracciones administrativas debe ser el de considerar que, salvo que quede acreditado lo contrario, el administrado no ha incurrido en los tipos declarados como tales infracciones. Y que esto es lo que se conoce como principio de presunción de inocencia, el cual es plenamente coherente con el hecho de que la Administración se encuentre obligada a llevar a cabo la actividad instructora para comprobar si una conducta concreta se subsume en un tipo infractor.

Cita, por lo que respecta a la presunción de inocencia, la Ley 39/2015 que en el procedimiento sancionador rige también dicho principio.

Cita también, respecto de la importancia de que el procedimiento administrativo respete el principio de tipicidad, la Sentencia del Tribunal Supremo de 2 de junio de 2010, Sala de lo Contencioso-Administrativo, Sección 4ª.

Indica la parte recurrente que, por lo que se refiere al principio de presunción de inocencia en el ámbito de la potestad administrativa sancionadora, la jurisprudencia ha sido igualmente unívoca en el sentido de exigir a los organismos administrativos un estricto respecto y sometimiento al mismo. Así, ya desde una temprana –y consolidada- doctrina, el Tribunal Constitucional ha venido declarando de manera invariable que el principio de presunción de inocencia sujeta plenamente la potestad sancionadora administrativa. Como ejemplo, cita -por todas- la Sentencia del Tribunal Constitucional 13/1982, de 1 de abril. Y cita también al Tribunal Supremo en su Sentencia de febrero 1994, Sala de lo Contencioso-Administrativo, Sección 7ª.

Estima la parte recurrente que ha sido sancionada por la comisión de unos hechos cuya existencia la AEPD no ha sido capaz de acreditar. Y que las pruebas que constan en el Expediente Administrativo, lejos de probar los hechos imputados, no acreditan nada más que el más estricto cumplimiento de la normativa de aplicación. Igualmente, la parte recurrente entiende que ha sido sancionada por la comisión de unos hechos imputados por la Agencia que no se ajustan al tipo infractor.

Por todos los argumentos expuestos, la parte recurrente considera que existe una ausencia total de elementos probatorios de la culpabilidad y, en consecuencia, una violación del derecho fundamental a la presunción de inocencia recogido en la Constitución Española.

Y que procede declarar la nulidad de la Resolución Sancionadora con base a lo establecido en el artículo 47 de la Ley 39/2015, en cuanto la misma vulnera los principios de tipicidad y presunción de inocencia, en concordancia con el artículo 24 de la Constitución Española.

Al respecto, esta Agencia desea reiterar lo ya expuesto en la citada Resolución Sancionadora objeto del presente recurso.

Al respecto, esta Agencia desea insistir en que se le imputó a la parte recurrente la comisión de las siguientes infracciones:

- Una infracción del artículo 13 del RGPD por no informar debidamente a los repartidores sobre la realización de decisiones individuales automatizadas (mediante la utilización del sistema "excellence score"): A lo largo del procedimiento sancionador ha quedado debidamente acreditado que la parte recurrente realizaba tales decisiones y que no informaba de ello debidamente a sus repartidores en los documentos pertinentes.

- También se le imputa la infracción de los artículos 25 y 32 del RGPD: En el presente caso, ha quedado debidamente acreditado a lo largo del procedimiento sancionador que la parte recurrente tenía implantado un sistema de permisos de acceso a los datos de los repartidores que no cumplía con las exigencias del artículo 32, toda vez que otorgaba acceso a datos que no eran necesarios para los fines otorgados. Y que tampoco actuó con diligencia por su parte a la hora de realizar un análisis adecuado previo al inicio del tratamiento sobre la información de los repartidores que debía facilitarse a los usuarios por ser necesaria para la consecución de los fines y la que debía quedar limitada por defecto.

Por todo lo expuesto, se desestima la presente alegación.

TERCERO-. PRESCRIPCIÓN DE LA INFRACCIÓN GRAVE DE LOS ARTÍCULOS 25 Y 32 DEL RGPD POR INAPLICABILIDAD DE LA DISPOSICIÓN ADICIONAL 4ª DEL REAL DECRETO 463/2020.

3.1. Cuestiones preliminares

Alega la parte recurrente que el *dies a quo* del plazo de prescripción de la infracción por vulneración de los artículos 25 y 32 del RGPD, debía fijarse el 18 de mayo de 2020, fecha en la que cesó la conducta presuntamente infractora mediante la implantación del "*sistema con acceso a los datos de los repartidores según los permisos habilitados por países y/o ciudades (city group permission)*". Teniendo en cuenta que el plazo de prescripción era de dos (2) años, el *dies ad quem* en el que se hubiese producido esta prescripción de la infracción sería el 18 de mayo de 2022. Y así la AEPD inicialmente coincidió con Glovo, tal como consta en la página 59 y siguientes de la Resolución Sancionadora objeto del presente recurso de reposición.

No obstante, la misma Resolución Sancionadora, en sus páginas 94 y siguientes, afirma que en ese momento estaba vigente la Disposición Adicional 4ª del *Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19* (en adelante "RD 463/2020"), la cual estableció la suspensión de los plazos de prescripción y caducidad de "*cualesquiera acciones y derechos*". Y que para ello, la AEPD se refiere a diversas resoluciones judiciales que avalarían la aplicación de esta Disposición

Adicional 4ª del RD 463/2020 al plazo de prescripción de las infracciones administrativas y, en consecuencia, de las que la referida Resolución Sancionadora trae causa.

De ser aplicable esa Disposición Adicional 4ª, el *dies a quo* no se hubiese iniciado hasta el 4 de junio de 2020, fecha en la que dejó de estar vigente dicha suspensión. Siendo ello así, el *dies ad quem* de la prescripción de la infracción se hubiese producido el 4 de junio de 2022. No obstante, el proyecto de acuerdo de inicio del PS/209/2022 se notificó a GLOVO el 27 de mayo de 2022, antes de que se hubiese producido la prescripción de la infracción.

Al respecto, esta Agencia desea señalar que coincide con la parte recurrente en que el *dies a quo* del plazo de prescripción de la infracción por incumplimiento de los artículos 25 y 32 del RGPD debería fijarse el 18 de mayo de 2020, siendo el *dies ad quem* del plazo de prescripción de dos años el 18 de mayo de 2022. Y que, tal como establece el artículo 95.3 de la LPACAP, la caducidad del procedimiento PS/00020/2021 no ha interrumpido el plazo de prescripción de la infracción en cuestión.

No obstante, el artículo 64 de la LOPDGDD "*Forma de iniciación del procedimiento y duración*" en su apartado 2 dispone:

"(…)
2. Cuando el procedimiento tenga por objeto la determinación de la posible existencia de una infracción de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, se iniciará mediante acuerdo de inicio adoptado por propia iniciativa o como consecuencia de reclamación.
(…)
Cuando fuesen de aplicación las normas establecidas en el artículo 60 del Reglamento (UE) 2016/679, el procedimiento se iniciará mediante la adopción del proyecto de acuerdo de inicio de procedimiento sancionador, del que se dará conocimiento formal al interesado a los efectos previstos en el artículo 75 de esta ley orgánica."

En este sentido, el artículo 75 "*Interrupción de la prescripción de la infracción"* de la LOPDGDD establece:

"(…)
Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679 interrumpirá la prescripción el conocimiento formal por el interesado del proyecto de acuerdo de inicio que sea sometido a las autoridades de control interesadas".

Por su parte, la Disposición adicional cuarta "*Suspensión de plazos de prescripción y caducidad*" del Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 dispuso que:

"Los plazos de prescripción y caducidad de cualesquiera acciones y derechos quedarán suspendidos durante el plazo de vigencia del estado de alarma y, en su caso, de las prórrogas que se adoptaren."

Y el artículo 10 "*Plazos de prescripción y caducidad de derechos y acciones suspendidos en virtud del Real Decreto 463/2020, de 14 de marzo***"** del Real Decreto 537/2020, de 22 de mayo, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 estableció que:

"Con efectos desde el 4 de junio de 2020, se alzará la suspensión de los plazos de prescripción y caducidad de derechos y acciones".

En el presente caso, se trata de un procedimiento sancionador en el que la AEPD ostenta la condición de autoridad de control principal, por tratarse de un tratamiento transfronterizo que realiza una empresa (la parte recurrente) que tiene su establecimiento principal en España y presta servicios a varios países de la Unión Europea, por lo que resulta de aplicación las normas establecidas en el artículo 60 del RGPD. Por tanto, es la adopción del proyecto de acuerdo de inicio de procedimiento sancionador el que da inicio al presente procedimiento e interrumpe la prescripción de la infracción el conocimiento formal del proyecto de acuerdo de inicio por parte de la parte recurrente.

Según consta en el expediente, el proyecto de acuerdo de inicio del procedimiento sancionador en cuestión se adoptó el 18 de mayo de 2022 y fue notificado a la parte recurrente el 27 de mayo de 2022.

Por tanto, siendo el *dies ad quem* del plazo de prescripción de dos años el 18 de mayo de 2022, pero teniendo en cuenta que debido a la situación excepcional a que dio lugar el COVID-19 se suspendieron tanto los plazos de prescripción como de caducidad desde el 14 de marzo de 2020 hasta el 1 de junio de 2020, la infracción de los artículos 25 y 32 del RGPD no estaba prescrita, toda vez que el *dies ad quem* del plazo de prescripción de dos años por la infracción de los artículos 25 y 32 el RGPD habría finalizado el 4 de junio de 2022.

Dado que el proyecto de acuerdo de inicio del procedimiento sancionador fue notificado a la parte recurrente el 27 de mayo de 2022, tal infracción no estaba prescrita.

Por todo lo expuesto, se desestima la presente alegación.

3.2. Irrelevancia de los antecedentes judiciales citados por la resolución sancionadora al no referirse a la cuestión objeto de discusión.

Alega la parte recurrente que, en primer lugar, el *quid* de la cuestión objeto de discusión es determinar si la Disposición Adicional 4ª del RD 463/2020 ha suspendido o no el plazo de prescripción de las infracciones administrativas y, en particular, la presunta infracción de los artículos 25 y 32 del RGPD que la referida Resolución Sancionadora trae causa. Y que no existe un pronunciamiento consolidado del Tribunal Supremo que haya resuelto esta cuestión.

Al respecto, esta Agencia desea señalar que sí que existe un pronunciamiento del Tribunal Supremo, que ya fue citado en la Resolución Sancionadora objeto del

presente recurso, la Sentencia núm. 1.509/2022 de 16 de noviembre, de la Sala de lo Contencioso-Administrativo, Sección Quinta, la cual en lo que aquí interesa expone:

"En lo que ahora importa, la cuestión de interés casacional suscitada tiene que ver con el contenido de las disposiciones adicionales tercera y cuarta. Conviene, pues, reproducir el contenido de las mencionadas Disposiciones adicionales:

"Disposición adicional tercera. Suspensión de plazos administrativos.
1. Se suspenden términos y se interrumpen los plazos para la tramitación de los procedimientos de las entidades del sector público. El cómputo de los plazos se reanudará en el momento en que pierda vigencia el presente real decreto o, en su caso, las prórrogas del mismo.
2. La suspensión de términos y la interrupción de plazos se aplicará a todo el sector público definido en la Ley39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
3. No obstante lo anterior, el órgano competente podrá acordar, mediante resolución motivada, las medidas de ordenación e instrucción estrictamente necesarias para evitar perjuicios graves en los derechos e intereses del interesado en el procedimiento y siempre que éste manifieste su conformidad, o cuando el interesado manifiestesu conformidad con que no se suspenda el plazo.
4. La presente disposición no afectará a los procedimientos y resoluciones a los que hace referencia el apartado primero, cuando estos vengan referidos a situaciones estrechamente vinculadas a los hechos justificativos del estado de alarma."

"Disposición adicional cuarta. Suspensión de plazos de prescripción y caducidad.
Los plazos de prescripción y caducidad de cualesquiera acciones y derechos quedarán suspendidos durante el plazo de vigencia del estado de alarma y, en su caso, de las prórrogas que se adoptaren."

Del tenor de la Disposición adicional tercera cabe deducir que la regla general establecida como consecuencia necesaria de la declaración de estado de alarma es la suspensión de los plazos establecidos para la tramitación de los procedimientos de las entidades del sector público (que son aquellas a las que se refiere el artículo 2 de la Ley 40/2015).

Ahora bien, conviene precisar que, aunque la suspensión sea la regla general, la propia Disposición se encarga de restringir la operatividad de esta regla general de dos maneras: por un lado, previendo su no aplicación a los procedimientos y resoluciones mencionados en el apartado 4; y, por otro, permitiendo en su apartado 3 que el órgano competente pueda acordar, mediante resolución motivada, las medidas de ordenación e instrucción estrictamente necesarias para evitar perjuicios graves en los derechos e intereses del interesado en el procedimiento y siempre que éste manifieste su conformidad, o cuando el interesado manifieste su conformidad con que no se suspenda el plazo.

Y, por otro lado, a la hora de interpretar los preceptos y disposiciones del Real Decreto para determinar el alcance de las consecuencias de su eventual incumplimiento, conviene tener muy presente la finalidad perseguida por éste, que - como hemos dichos antes- es la protección de la seguridad jurídica y de los derechos e intereses legítimos de los ciudadanos.

Por ello, que la regla general sea la procedencia de suspender los plazos de tramitación no significa que esté vedada toda posibilidad de actuación administrativa mientras dure la vigencia del estado de alarma o de sus prórrogas. La norma no establece la paralización de la actividad administrativa o, más precisamente, de la paralización de la actividad de las entidades del sector público (como tampoco se refiere a la paralización de la actividad de los órganos judiciales del país), debiendo tenerse en cuenta a este respecto que, esa consecuencia, aparte de no acomodarse a la finalidad perseguida por la norma, habría podido generar, eventualmente, graves perjuicios para el interés general y para los concretos derechos e intereses de los ciudadanos.

Por ello, cabe colegir que lo que realmente se pretende con el citado Real Decreto es que, para protegerlos derechos de los ciudadanos, la eficacia de esas actuaciones administrativas -que no deben reputarse necesariamente inválidas por haberse realizado durante ese periodo- quedará en suspenso, esto es, que su eficacia se verá demorada hasta que cese el estado de alarma -cuya duración fijaba en quince días naturales el artículo 3 del Real Decreto- o sus prórrogas, reanudándose entonces el cómputo de los plazos.

Y este mismo razonamiento es aplicable a la Disposición adicional cuarta, que dispone que los plazos de prescripción y caducidad de cualesquiera acciones y derechos quedarán suspendidos durante el plazo de vigencia del estado de alarma y, en su caso, de las prórrogas que se adoptaren.

Por tanto, la notificación de una resolución sancionadora dictada con anterioridad a la declaración del estado de alarma, que hubiera sido practicada durante la vigencia de éste o de sus prórrogas, no puede reputarse -en principio- inválida, sin perjuicio de que su eficacia quede demorada hasta el momento de la cesación del estado de alarma o de sus prórrogas, a partir del cual se reanudará el cómputo de los plazos. Y, en línea con lo expuesto, también durante ese periodo de vigencia del estado de alarma o de sus prórrogas quedará en suspenso el plazo de caducidad de cualesquiera acciones o derechos.

En consecuencia, podemos dar respuesta a la cuestión de interés casacional planteada en el auto de admisión en los siguientes términos:

(i) La Disposición adicional tercera del Real Decreto 463/2020, debe ser interpretada en el sentido de que la notificación de una resolución sancionadora dictada con anterioridad a la declaración del estado de alarma, y practicada durante la vigencia de éste, debe reputarse -en principio- válida, sin perjuicio de que su eficacia quede demorada hasta el momento de la cesación del estado de alarma o de sus prórrogas, a partir del cual se reanudará el cómputo de los plazos.

(ii) Y, en línea con lo expuesto, la Disposición adicional cuarta del citado Real Decreto debe ser interpretada en el sentido de que durante el periodo de vigencia del estado de alarma o de sus prórrogas quedará en suspenso el plazo de caducidad de cualesquiera acciones o derechos y, por tanto, también de aquéllos a los que se refería la notificación antes indicada."

Continúa alegando la parte recurrente que, para justificar la aplicación de la Disposición Adicional 4ª del RD 463/2020, la Resolución Sancionadora cita diversas resoluciones judiciales que avalarían, supuestamente, la posición de la AEPD.

Alega la parte recurrente que el fragmento citado de la Sentencia del Tribunal Superior de Justicia de Aragón (Sala de lo Contencioso-Administrativo, Sección 2ª), núm. 290/2022, de 14 de octubre (JUR 2022\376138) -véase página 96 de la Resolución Sancionadora-, se refiere a la caducidad del procedimiento sancionador en aplicación de la Disposición Adicional 3ª del RD 463/2020, y no a la prescripción de la infracción (que también es alegada y estimada, pero por otros motivos que nada tienen que ver con la aplicación del RD 463/2020).

Al respecto esta Agencia desea recordar el citado fragmento a que refiere la parte recurrente:

"(…)
Y respecto a las alegaciones de la parte sobre la vigencia de los principios de funcionamiento de las administraciones públicas, la habilitación de medidas organizativas de teletrabajo para posibilitar la prestación de los servicios de las personas empleadas públicas en remoto, el ser extremadamente cauteloso en el caso de notificaciones con suspensión de plazos, procurando, en la medida de lo posible, evitar causar perjuicios derivados de interpretaciones confusas en cuanto a dicha cuestión, y la mención de la parte a las actuaciones seguidas por la Administración durante el Estado de Alarma, bastará recordar la situación que vivía el país en esas fechas, con intensas limitaciones de derechos motivadas por una grave crisis sanitaria que se transmitió a toda la sociedad española y que dificultó la actividad social e institucional, situación en la que fue necesario aprobar normas para hacer frente a esas dificultades, aportando seguridad jurídica en las relaciones de los ciudadanos con las Administraciones Públicas. El plazo de suspensión, que alcanzó los 78 días, protegió a los ciudadanos de los efectos indeseables de posibles preclusiones de plazos y estableció el marco jurídico que debía regir los plazos de prescripción y caducidad, marco que debemos entender vigente en el apartado que examinamos de una alegación de caducidad". (el subrayado es de la Agencia)

En este sentido, esta Agencia entiende que el hecho de que se estuviera contestando a una alegación sobre caducidad no obsta a que la misma sentencia haga referencia también a los plazos de prescripción, debido a la suspensión de los plazos tanto de prescripción como de caducidad que realizó el citado Real Decreto, motivada por la situación excepcional de "grave crisis sanitaria que se transmitió a toda la sociedad española que dificultó la actividad social e institucional".

Alega también la parte recurrente que la Sentencia del Tribunal Superior de Justicia de Madrid (Sala de lo Contencioso-Administrativo, Sección 10ª) núm. 68/2023, de 17 de enero (JUR 2023\51556), también se refiere a la aplicación de la Disposición Adicional 3ª del RD 463/2020, sin que pueda extenderse este pronunciamiento a la aplicación de la Disposición Adicional 4ª.

Al respecto, esta Agencia desea recordar el citado fragmento a que refiere la parte recurrente:

"*Como se observa por el Abogado del Estado y aunque resulte irrelevante, incurre la resolución apelada en un error material. Ello al expresar que hubo dos intentos fallidos en la notificación de la expulsión. Lo cierto es que, como el propio apelado admite y se desprende del expediente [folio 31], tras un primer intento de notificación el 7/6/21 en el que el apelado se encontraba ausente, el 8/6/21 tuvo lugar la notificación, constando su rúbrica en el acuse de recibo.*

A partir de ahí, debe tenerse en cuenta que el inicio del procedimiento se produce el 19/2/20 y que deviene decisivo para entender o no transcurrido el plazo de caducidad los efectos que se le otorguen a la suspensión de plazos dispuesta por la Disposición Adicional Tercera del Real Decreto 463/2020, de 14 de marzo , por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, en relación con el artículo 9 del Real Decreto 537/2020, de 22 de mayo , por el que se prorroga el estado de alarma.

La tesis por la que se decanta la Sentencia es que tal suspensión no puede operar en perjuicio del administrado. Interpreta al efecto que la suspensión implicaba una ampliación desfavorable para el ciudadano y contraria al artículo 9.3 de la Constitución. Por su parte, el Abogado del Estado atinadamente subraya que lo que en realidad está haciendo la Juzgadora de instancia es inaplicar una disposición con rango y valor de ley sin, como resultaría preceptivo, promover la cuestión de inconstitucionalidad ex artículo 163 de la Constitución.

Se trata esta de una cuestión sobre la que ya ha tenido la ocasión de pronunciarse esta Sala y Sección [por todas, Sentencia Nº 776/2022, de 3 de octubre (rec. 839/2021)]. Como en la misma se expresaba, " no cabe considerar de una manera unívoca e indiscutible que la citada Disposición Adicional Tercera se trate de una disposición sancionadora desfavorable o restrictiva de derechos individuales, dado que su objetivo no es limitar o restringir derechos sino salvaguardar el derecho de los ciudadanos a relacionarse con las Administraciones Públicas y el normal ejercicio por parte de las Administraciones Públicas en sus relaciones con los ciudadanos ante las dificultades para el normal ejercicio de esos derechos y potestades derivadas de las limitaciones a la libertad de circulación de las personas y las demás medidas excepcionales contenidas en el Real Decreto-Ley. La aplicación de la suspensión de plazos administrativos establecida en el Real Decreto 462/2020, a través de la Disposición Adicional Tercera, resulta aplicable a los procedimientos sancionadores o restrictivos de derechos individuales iniciados antes de la declaración del estado de alarma y pendientes de resolución en el momento de la entrada en vigor de la referida norma legal, produce efectos favorables para los ciudadanos afectados " [F.D. 2º].

Consiguientemente y por mor de la aplicación de la Disposición Adicional Tercera del Real Decreto 463/2020, de 14 de marzo, no cabe afirmar que se haya producido la caducidad del expediente de expulsión por haber sido notificada la resolución de expulsión una vez transcurridos seis meses desde la fecha de inicio de dicho procedimiento.

Se sigue de lo anterior la estimación del recurso de apelación y la consiguiente revocación de la Sentencia. Ello, a su vez, se ha de traducir en la desestimación del recurso deducido en la instancia, confirmándose la actuación administrativa impugnada.

Al respecto, esta Agencia desea señalar que esta sentencia no fue citada en las alegaciones referidas únicamente a la prescripción de la infracción sino para contestar en concreto a la alegación esgrimida por la parte recurrente de que no podría aplicarse dicho precepto porque sería contrario, entre otros, al artículo 9.3 de la Constitución relativo a la irretroactividad de las disposiciones sancionadoras no favorables o restrictivas de derechos individuales. Y esta Agencia trajo a colación tal sentencia dado que, si bien analiza la Disposición adicional tercera de tal Real Decreto, podría hacerse extensible sus conclusiones a la Disposición adicional cuarta del Real Decreto en cuestión, toda vez que no puede interpretarse que el Real Decreto se trate de una disposición sancionadora desfavorable o restrictiva de derechos individuales.

Indica la parte recurrente que el razonamiento de las anteriores sentencias citadas por la Resolución Sancionadora no debería entenderse aplicable al caso de Glovo, puesto que no es lo mismo entender que el plazo para tramitar los procedimientos (cualesquiera que sean) quedan interrumpidos que hacer una interpretación extensiva de los términos "*cualesquiera acciones y derechos*" recogidos en la Disposición Adicional 4ª para incluir en el supuesto de suspensión el plazo de prescripción de las infracciones.

Por tanto, explica la parte recurrente que no deben confundirse ambas disposiciones, pues mientras la Disposición Adicional 3ª trata de la interrupción de los plazos para la tramitación de los procedimientos, la Disposición Adicional 4ª se refiere a la suspensión de los plazos de prescripción y caducidad de cualesquiera acciones y derechos.

Y, añade que así lo afirma la Audiencia Provincial de Badajoz (Sección 2ª), en su Sentencia núm. 822/2021, de 22 octubre (JUR 2022\29414). Según dicho órgano judicial deben entenderse como supuestos plenamente diferenciados:

"*Y la disposición adicional cuarta del Real Decreto 463/ 2020, sobre suspensión de plazos de prescripción y caducidad, es del siguiente tenor: <<Los plazos de prescripción y caducidad de cualesquiera acciones y derechos quedarán suspendidos durante el plazo de vigencia del estado de alarma y, en su caso, de las prórrogas que se adoptaren>>.*

Pues bien, esta otra norma solo concierne a los plazos de prescripción y de caducidad establecidos para el ejercicio de derechos, no a los plazos de duración de los procedimientos. Estamos ante supuestos bien distintos. Alcanza solo a los plazos sustantivos de ejercicio de los derechos. Y no hay lugar a la confusión, porque el propio legislador, en la disposición tercera, tuvo a bien contemplar explícitamente la suspensión de plazos administrativos".

Al respecto, esta Agencia coincide en que la disposición adicional cuarta del Real Decreto 463/2020 no refiere a los plazos de duración de los procedimientos, no suspende los plazos administrativos, sino que se trata de que ha quedado suspendido el plazo de prescripción de las infracciones que pueden perseguirse por vía administrativa.

Por otro lado, añade la parte recurrente que por lo que respecta a la Sentencia del Tribunal Supremo (Sala de lo Contencioso-Administrativo, Sección 5ª), núm. 1509/2022, de 16 de noviembre (JUR 2022\360086), es relevante destacar que en ella el Tribunal Supremo no se refiere a la prescripción de la infracción, sino, nuevamente, a la caducidad del procedimiento sancionador, y su referencia a la Disposición Adicional 4ª solamente es a los efectos de afirmar la interrupción del plazo de prescripción de los derechos y acciones que otorga la notificación de la resolución sancionadora, y no de la prescripción de la infracción en sí misma considerada.

En palabras del Alto Tribunal:

"*Por tanto, la notificación de una resolución sancionadora dictada con anterioridad a la declaración del estado de alarma, que hubiera sido practicada durante la vigencia de éste o de sus prórrogas, no puede reputarse -en principio- inválida, sin perjuicio de que su eficacia quede demorada hasta el momento de la cesación del estado de alarma o de sus prórrogas, a partir del cual se reanudará el cómputo de los plazos. Y, en línea con lo expuesto, también durante ese periodo de vigencia del estado de alarma o de sus prórrogas quedará en suspenso el plazo de caducidad de cualesquiera acciones o derechos.* [...]

(ii) Y, en línea con lo expuesto, la Disposición adicional cuarta del citado Real Decreto debe ser interpretada en el sentido de que durante el periodo de vigencia del estado de alarma o de sus prórrogas quedará en suspenso el plazo de caducidad de cualesquiera acciones o derechos y, por tanto, también de aquéllos a los que se refería la notificación antes indicada." (el destacado es de Glovo)

Al respecto, esta Agencia no coincide con la interpretación que realiza la parte recurrente de esta última sentencia en cuestión, tal como fue indicado en la citada Resolución Sancionadora.

En cualquier caso, la sentencia que se esgrime refiere a un supuesto de hecho diferente al presente, toda vez que su objeto es la notificación de una resolución de un procedimiento dictada antes de que se declare el citado estado de alarma y notificado después de su declaración; mientras que en el presente caso se trata de la notificación de un acto dictado una vez finalizado tal estado de alarma y que da inicio a un procedimiento sancionador, cuya notificación interrumpe la prescripción de la infracción en cuestión, que es el supuesto que nos ocupa en el presente recurso.

Así las cosas, y teniendo en cuenta todo lo anterior, concluye la parte recurrente lo siguiente:

I. La mayoría de los pronunciamientos citados en la Resolución Sancionadora no resuelven la cuestión controvertida en este caso: si la Disposición Adicional 4ª del RD 463/2020 afectó o no al plazo de prescripción de las infracciones administrativas.

II. Sobre esta cuestión solamente existen algunos pronunciamientos de órganos unipersonales, de carácter contradictorio, sin que sea una materia sobre la que el Tribunal Supremo haya establecido una doctrina consolidada.

Al respecto, esta Agencia desea señalar que además de las reseñadas sentencias por la parte recurrente (Sentencia núm. 290/2022 de 14 de octubre del Tribunal Superior de Justicia de Aragón y Sentencia del Tribunal Superior de Justicia de Madrid, (Sala de lo Contencioso-Administrativo), núm. 68/2023 de 17 de enero, esta última solo a efectos de la alegación sobre irretroactividad de las disposiciones sancionadoras no favorables o restrictivas de derechos individuales), en la Resolución Sancionadora objeto del presente recurso se cita también otras tres sentencias: Sentencia núm. 189/2021 de 30 de octubre, del Juzgado de lo Contencioso-Administrativo N. 3 de Toledo y Sentencia núm. 401/2022 de 14 de julio, del Tribunal Superior de Justicia de Murcia, (Sala de lo Contencioso-Administrativo, Sección 2ª), que resultan plenamente aplicables a la presente cuestión, además de la Sentencia núm. 1.509/2022 de 16 de noviembre del Tribunal Supremo, Sala de lo Contencioso-Administrativo, Sección Quinta.

En especial, esta Agencia destacar la Sentencia núm. 189/2021 de 30 de octubre del Juzgado de lo Contencioso-Administrativo N. 3 de Toledo, que ha entendido que:

"*3.- Prescripción de la infracción.*
(…)
No obstante lo anterior, en el presente caso, deben ser tenidas en cuenta las especiales circunstancias acaecidas con ocasión del COVID, que provocaron que por Real Decreto 463/2020, de 14 de Marzo se declarara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, cuya Disposición Adicional 4.ª "Suspensión de plazos de prescripción y caducidad.", señaló que "Los plazos de prescripción y caducidad de cualesquiera acciones y derechos quedarán suspendidos durante el plazo de vigencia del estado de alarma y, en su caso, de las prórrogas que se adoptaren.", si bien el Real Decreto 537/2020, de 22 de Mayo, que prorrogó el estado de alarma, en su Artículo 9 señaló que con efectos desde el 1 de Junio de 2020 el cómputo de los plazos administrativos que hubieran sido suspendidos se reanudará, o se reiniciará, y en su Artículo 10 que con efectos desde el 4 de Junio de 2020 se alzará la suspensión de los plazos de prescripción y caducidad de derechos y acciones.

En el caso que nos ocupa al tiempo de declararse el estado de alarma el procedimiento sancionador no se encontraba incoado, suspendiéndose por tanto desde el 14 de Marzo de 2020 hasta el 4 de Junio de 2020 el plazo de prescripción de la infracción, de modo que cometida ésta el 22 de Junio de 2019, suspendiéndose el plazo de prescripción de la infracción el 14 de Marzo de 2020, alzándose la referida suspensión con fecha 4 de Junio de 2020, fecha coincidente con el acuerdo de iniciación del expediente, que concluyó con el dictado de la Resolución sancionadora de 16 de Octubre de 2020, notificada al interesado el día 30 del mismo mes y año, se considera que la infracción no había prescrito, decayendo la alegación realizada por la recurrente en este aspecto".

Esto significa que en la Resolución Sancionadora se citaron sobre la cuestión que nos ocupa en concreto cuatro sentencias, tres de las cuales no han sido controvertidas por la parte recurrente, más allá de que en aquello que se recurre esta Agencia no comparta su criterio. Por tanto, no se trata de que en el presente caso "la mayoría de los pronunciamientos citados en la Resolución Sancionadora no resuelven la cuestión

controvertida en este caso", sino que por el contrario, sería casi la totalidad de estos pronunciamientos los que avalarían la postura de esta Agencia.

Finalmente, alega la parte recurrente que "sobre esta cuestión solamente existen algunos pronunciamientos de órganos unipersonales, de carácter contradictorio, sin que sea una materia sobre la que el Tribunal Supremo haya establecido una doctrina consolidada". Sin embargo, únicamente una de las sentencias citadas por la Resolución Sancionadora es de un órgano unipersonal, mientras que las otras tres son órganos colegiados, de hecho se trata de dos Tribunales Superiores de Justicia y una sala del Tribunal Supremo.

Por todo lo expuesto, se desestima la presente alegación.

3.3. Aplicación de los mismos principios del derecho penal al derecho administrativo sancionador. La Disposición Adicional 4ª del RD 463/2020 no suspende la prescripción de los delitos.

Alega la parte recurrente que en el ámbito penal, las distintas Audiencias Provinciales han entendido (con base en las Sentencias del Tribunal Constitucional núm. 63/2005, de 14 de marzo y núm. 12/1991, de 28 de enero) que la Disposición Adicional 4ª del RD 463/2020 no es aplicable a la prescripción de los delitos, ya que lo que prescribe es el delito en sí, no la acción procesal para perseguir estos delitos.

Y que en este sentido, la Sentencia de la Audiencia Provincial de Murcia (Sección 3ª) núm. 101/2022, de 18 de febrero de 2022, dictada en el recurso de apelación núm. 77/2021 (JUR 2022\141487), afirma que:

"*No obstante, la prescripción del delito no debe ser confundida con la prescripción de acciones y derechos a la que alude el RD 463/2020 de 14 de marzo por el que se declaraba el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, por tratarse de instituciones de distinta naturaleza jurídica. Si bien, es cierto que la norma precitada supuso la interrupción de los plazos de prescripción y caducidad de cualesquiera acciones o derecho por disponerlo así la mencionada Disposición Adicional 4ª del Decreto 463/2020 , pero no la interrupción de los plazos de prescripción de los delitos*". (el destacado es de Glovo)

En un sentido parecido, la parte recurrente cita la SAP de Tarragona (Sección 2ª) núm. 134/2021, de 9 de abril de 2021, dictada en el recurso de apelación 25/2021, que dispone que:

"*Por lo tanto el Real Decreto que viene a habilitar el estado de alarma, tan solo se está refiriendo a la prescripción de " cualesquiera acciones y derechos", es decir al ejercicio de la acción penal (bien sea mediante denuncia y personación o mediante querella) sin que se haga mención a los delitos y sus consecuencias sancionadoras. Ello nos lleva a considerar que los delitos (y por lo tanto su prescripción) estarían fuera de la regla general de suspensión que regula el indicado Real Decreto*."

Por último, la parte recurrente cita la SAP de Guadalajara (Sección 1ª) núm. 241/2022, de 1 diciembre de 2022, dictada en el recurso de apelación núm. 818/2022 (JUR 2023\10815), que ha resuelto lo siguiente:

"*No obstante, se considera que la prescripción del delito no debe ser confundida con la prescripción de acciones y derechos a la que alude el RD 463/2020, de 14 de marzo, por el que se declaraba el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, por tratarse de instituciones de distinta naturaleza jurídica. La disposición adicional cuarta alude a los "plazos de prescripción y caducidad de cualesquiera acciones y derechos", pero la prescripción del delito no se configura como un derecho de parte al ejercicio de la acción penal durante un plazo concreto, sino como una potestad del Estado a poner límites al ius puniendi, lo que se vincula con la naturaleza eminentemente sustantiva o material del instituto de la prescripción del delito, en detrimento de una naturaleza de carácter procesal*." (el destacado es de Glovo)

Asimismo, indica la parte recurrente que esta interpretación relativa a la no aplicación de la Disposición Adicional 4ª del RD 463/2020 a la prescripción de delitos también fue sostenida por la Fiscalía General del Estado en su Informe de 3 de junio de 2020 del Fiscal de Sala Jefe de la Secretaría Técnica de la Fiscalía General del Estado sobre la prescripción de los delitos durante el estado de alarma.

"*De ahí que resulte incontrovertida la imposibilidad de aplicar las previsiones que se contienen en la D.A. 4ª del RD 463/2020, de 14 de marzo, acerca de la suspensión de los plazos de prescripción y caducidad para el ejercicio de acciones y derechos, a los plazos de prescripción del delito regulados por el artículo 131 CP. Pues, en este último caso, lo que prescribe no es la acción penal para perseguir el delito sino el delito mismo.*" (el destacado es de Glovo)

En este contexto, explica la parte recurrente que tanto el derecho penal como el derecho administrativo sancionador forman parte del *ius puniendi* del Estado. Y cita, por todas, a la Sentencia del Tribunal Constitucional núm. 18/1981, de 8 de junio, así como la Sentencia del Tribunal Supremo (Sala de lo Contencioso-Administrativo, Sección 5ª) núm. 2118/1996, de 9 de abril, dictada en el recurso núm. 6373/1991 (RJ 1996\3375).

Y que esta última ha resuelto lo siguiente:

"*Esta Sala, a través de reiterada jurisprudencia, viene sosteniendo que la teoría general del ilícito como supraconcepto comprensivo tanto del penal como del administrativo establece que la potestad sancionadora de la Administración ha de ejercitarse ajustándose a los principios esenciales inspiradores del orden penal, ya que dicha potestad tiene como soporte teórico la negación de cualquier diferencia ontológica entre sanción administrativa y pena.*

También el Tribunal Constitucional en Sentencias de 21 enero 1987 (RTC 1987\2) y 6 febrero 1989 (RTC 1989\29) ha declarado que los principios inspiradores del orden penal son de aplicación con ciertos matices al Derecho Administrativo sancionador dado que ambos son manifestaciones del ordenamiento punitivo del Estado, y ello tanto en un sentido material como procedimental, y por ello, es necesario para la imposición de una sanción, la constancia clara e individualizada de la autoría de los hechos determinantes de la sanción así como de la antijuridicidad tipificada de los mismos y su imputación culposa o dolosa." (el destacado es de Glovo)

Alega la parte recurrente que, si en el ámbito penal lo que prescriben son los delitos en sí, no las acciones para perseguir esos delitos, esta misma conclusión debe aplicarse en el ámbito administrativo, en el que prescriben las infracciones en sí mismas consideradas, no la "acción" de la Administración para sancionar estas infracciones.

Indica la parte recurrente que el artículo 30 de la LRJSP no deja lugar a dudas, ya que, como sucede en el ámbito penal, habla del "*plazo de prescripción de las infracciones*", no del plazo de prescripción de una acción para sancionar infracciones.

"[...]
2. El plazo de prescripción de las infracciones comenzará a contarse desde el día en que la infracción se hubiera cometido. En el caso de infracciones continuadas o permanentes, el plazo comenzará a correr desde que finalizó la conducta infractora.
[....]"

Explica la parte recurrente que esta misma expresión se utiliza por los artículos 72 a 74 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, la "LOPDGDD"), los cuales prevén que "*prescribirán a los* [...] *años las infracciones*".

"Artículo 72. Infracciones consideradas muy graves.
1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:
[...]

Artículo 73. Infracciones consideradas graves.
En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:
[...]

Artículo 74. Infracciones consideradas leves.
Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679 y, en particular, las siguientes:
[...]"

Alega la parte recurrente que siendo ello así, y a pesar de que no existe a día de hoy una jurisprudencia consolidada del Tribunal Supremo que fije doctrina sobre esta cuestión, se debe concluir que el plazo de prescripción de las infracciones no ha quedado afectado por la Disposición Adicional 4ª del RD 463/2020, ya que lo que prescriben son las infracciones en sí mismas, no las acciones para perseguirlas.

Al respecto, esta Agencia simplemente se limita a señalar que toda esta alegación hace referencia a la prescripción de delitos en el ámbito penal, mientras que en el presente caso se está en el ámbito administrativo, que es el que regula la citada

Disposición Adicional 4ª del RD 463/2020. Además, la citada norma no puede interpretarse en el sentido propuesto por la parte recurrente, ya que si se adoptase tal interpretación todas las infracciones habría prescrito en el citado período por el mero transcurso del plazo toda vez que la Administración estaba atada sin poder perseguirlas

Por todo lo expuesto, se desestima la presente alegación.

3.4. Vulneración del principio de seguridad jurídica y al principio de irretroactividad de las disposiciones sancionadoras no favorables por indebida aplicación de la Disposición Adicional 4ª del RD 463/2020 al plazo de prescripción de las infracciones administrativas.

Alega la parte recurrente que la aplicación de la Disposición Adicional 4ª a la prescripción de infracciones sería contraria al principio de seguridad jurídica y la interdicción de la retroactividad de las disposiciones sancionadoras no favorables o restrictivas de derechos, recogida en el artículo 9.3 de la Constitución Española.

Cita la Sentencia de la Audiencia Provincial de Guadalajara (Sección 1ª, núm. 241/2022, de 1 diciembre de 2022:

"*Asumir que la disposición adicional cuarta del R.D 463/2020 tuviera efectividad en esta materia, afectaría a unos fundamentos materiales de la prescripción del delito, como es el principio de seguridad jurídica tal y de legalidad penal, que exige que quién presuntamente ejecute una conducta delictiva sea enjuiciado conforme a la normativa vigente al tiempo de los hechos, tanto en cuando a la tipificación penal del delito como a las causas que generen la extinción de su responsabilidad, sin que la normativa posterior le afecte, salvo que resulte más favorable, proscribiendo el legislador constitucional la hipótesis contraria al garantizar el principio de irretroactividad de las normas sancionadoras no favorables (art. 9.3 de la Constitución). Como señala la STS 613/2003 de 20 de junio (RJ 2003, 6869) (EDJ 2003/97963) "coincide últimamente jurisprudencia y doctrina en considerar que el instituto de la prescripción es de naturaleza material y no procesal, lo que determina como consecuencia que las modificaciones legislativas de los plazos o condiciones de la prescripción serán irretroactivas si perjudican al reo y retroactivas si le son favorables.*

Se aplicarán, por tanto, en principio a la prescripción las normas penales vigentes cuando empieza a operar tal causa de extinción de la responsabilidad penal, que se inicia en la fecha de la comisión del delito o en la de paralización del procedimiento por causa de rebeldía. Las normas penales posteriores sobre prescripción operaran si resultan más favorables al reo". (el destacado es de Glovo)

Alega la parte recurrente que las anteriores consideraciones deben extenderse al ámbito del derecho administrativo sancionador, el cual se rige por los mismos principios que el derecho penal, ya que ambos son manifestaciones del *ius puniendi*.

Cita la parte recurrente la Sentencia del Juzgado Contencioso-Administrativo núm. 1 de Salamanca (Sección 1ª), núm. 135/2021, de 3 de junio, que se pronunció a favor de entender prescrita una sanción administrativa y consideró inaplicable la Disposición Adicional 4ª en base al principio de seguridad jurídica:

"*Sin embargo, estamos ante un procedimiento sancionador, la prescripción de la sanción, y a este respecto el artículo 9.3 de la Constitución sobre la "irretroactividad de las disposiciones sancionadoras no favorables o restrictivas de derechos individuales, la seguridad jurídica", impide que la suspensión declarada por el Real Decreto afecte al cómputo de la prescripción de la sanción, supondría una ampliación del plazo de prescripción aplicada retroactivamente*".

Alega la parte recurrente que dicha argumentación se puede extender plenamente al presente caso de Glovo en atención a ese mismo principio de seguridad jurídica en el que se cuestiona la aplicación a la prescripción de las infracciones administrativas.

Al respecto, esta Agencia desea reiterar lo ya expuesto en la respuesta a la anterior alegación.

Y reforzar con lo ya expuesto en la citada Resolución Sancionadora objeto del presente recurso.

En este sentido, esta Agencia desea traer a colación la Sentencia del Tribunal Superior de Justicia de Madrid, (Sala de lo Contencioso-Administrativo), num. 68/2023 de 17 de enero, que, si bien analiza la Disposición adicional tercera de tal Real Decreto, podría hacerse extensible sus conclusiones a la Disposición adicional cuarta del Real Decreto en cuestión, toda vez que no puede interpretarse que el Real Decreto se trate de una disposición sancionadora desfavorable o restrictiva de derechos individuales:

"*Como se observa por el Abogado del Estado y aunque resulte irrelevante, incurre la resolución apelada en un error material. Ello al expresar que hubo dos intentos fallidos en la notificación de la expulsión. Lo cierto es que, como el propio apelado admite y se desprende del expediente [folio 31], tras un primer intento de notificación el 7/6/21 en el que el apelado se encontraba ausente, el 8/6/21 tuvo lugar la notificación, constando su rúbrica en el acuse de recibo.*

A partir de ahí, debe tenerse en cuenta que el inicio del procedimiento se produce el 19/2/20 y que deviene decisivo para entender o no transcurrido el plazo de caducidad los efectos que se le otorguen a la suspensión de plazos dispuesta por la Disposición Adicional Tercera del Real Decreto 463/2020, de 14 de marzo , por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, en relación con el artículo 9 del Real Decreto 537/2020, de 22 de mayo , por el que se prorroga el estado de alarma.

La tesis por la que se decanta la Sentencia es que tal suspensión no puede operar en perjuicio del administrado. Interpreta al efecto que la suspensión implicaba una ampliación desfavorable para el ciudadano y contraria al artículo 9.3 de la Constitución. Por su parte, el Abogado del Estado atinadamente subraya que lo que en realidad está haciendo la Juzgadora de instancia es inaplicar una disposición con rango y valor de ley sin, como resultaría preceptivo, promover la cuestión de inconstitucionalidad ex artículo 163 de la Constitución.

Se trata esta de una cuestión sobre la que ya ha tenido la ocasión de pronunciarse esta Sala y Sección [por todas, Sentencia Nº 776/2022, de 3 de octubre (rec.

839/2021)]. Como en la misma se expresaba, " no cabe considerar de una manera unívoca e indiscutible que la citada Disposición Adicional Tercera se trate de una disposición sancionadora desfavorable o restrictiva de derechos individuales, dado que su objetivo no es limitar o restringir derechos sino salvaguardar el derecho de los ciudadanos a relacionarse con las Administraciones Públicas y el normal ejercicio por parte de las Administraciones Públicas en sus relaciones con los ciudadanos ante las dificultades para el normal ejercicio de esos derechos y potestades derivadas de las limitaciones a la libertad de circulación de las personas y las demás medidas excepcionales contenidas en el Real Decreto-Ley. La aplicación de la suspensión de plazos administrativos establecida en el Real Decreto 462/2020, a través de la Disposición Adicional Tercera, resulta aplicable a los procedimientos sancionadores o restrictivos de derechos individuales iniciados antes de la declaración del estado de alarma y pendientes de resolución en el momento de la entrada en vigor de la referida norma legal, produce efectos favorables para los ciudadanos afectados " [F.D. 2º].

Consiguientemente y por mor de la aplicación de la Disposición Adicional Tercera del Real Decreto 463/2020, de 14 de marzo, no cabe afirmar que se haya producido la caducidad del expediente de expulsión por haber sido notificada la resolución de expulsión una vez transcurridos seis meses desde la fecha de inicio de dicho procedimiento.

Se sigue de lo anterior la estimación del recurso de apelación y la consiguiente revocación de la Sentencia. Ello, a su vez, se ha de traducir en la desestimación del recurso deducido en la instancia, confirmándose la actuación administrativa impugnada.

Dado que no puede entenderse que la Disposición Adicional cuarta del Real Decreto 463/2020 se trate de una disposición sancionadora desfavorable o restrictiva de derechos individuales, no habría sido vulnerado el principio de seguridad jurídica ni el de irretroactividad de las disposiciones sancionadoras no favorables.

Por tanto, por todo lo expuesto, se desestima la presente alegación.

3.5. Anulabilidad de la sanción de 550.000 Euros por prescripción de la infracción de los artículos 25 y 32 del RGPD.

Explica la parte recurrente que, a su entender, teniendo en cuenta lo expuesto en los apartados anteriores, queda claro que la Disposición Adicional 4ª del RD 463/2020 no afectó al plazo de prescripción de la infracción por la supuesta vulneración de los artículos 25 y 32 del RGPD.

"*Como en el presente caso el dies ad quem de prescripción de dos años sería el 18 de mayo de 2022* [...]".

Alega la parte recurrente que el 18 de mayo de 2022 aún no se había producido la interrupción de la prescripción derivada de la incoación del procedimiento sancionador 209/2022. El proyecto de acuerdo de inicio de este procedimiento se dictó el 18 de mayo de 2022, pero no fue puesto a disposición de Glovo hasta el 19 de mayo de 2022, quién accedió a la notificación el 27 de mayo de 2022. Esta última fecha es en la cual se entiende practicada la notificación, según lo dispuesto en el artículo 43.2 de la

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Alega la parte recurrente que la interrupción de la prescripción se produce una vez se notifica el acuerdo de incoación de un procedimiento sancionador, no cuando este se dicta. Así lo dispone el artículo 30.2 de la LRJSP, cuando prevé que la prescripción se producirá cuando se inicie un procedimiento sancionador "*con conocimiento del interesado*":

"*Interrumpirá la prescripción la iniciación, con conocimiento del interesado, de un procedimiento administrativo de naturaleza sancionadora* [...]".

Y que el artículo 75 de la LOPDGDD dispone lo siguiente:

"*Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.*

Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679 interrumpirá la prescripción el conocimiento formal por el interesado del proyecto de acuerdo de inicio que sea sometido a las autoridades de control interesadas" (el resaltado es de Glovo).

Por todo lo anterior, la parte recurrente concluye que la infracción por vulneración de los artículos 25 y 32 del RGPD había prescrito en el momento en que se habría producido la interrupción de esta prescripción (el 27 de mayo de 2022, fecha de notificación del proyecto de acuerdo de inicio del procedimiento sancionador), ya que esta prescripción se produjo el 18 de mayo de 2022.

Y que la sanción impuesta por esta infracción debe ser anulada.

Al respecto, esta Agencia se reitera en lo ya expuesto tanto en la Resolución Sancionadora objeto del presente recurso como en la presente resolución.

Esta Agencia se reitera en que la Disposición adicional cuarta del *Real Decreto de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19* resulta de aplicación al presente supuesto.

El artículo 64 de la LOPDGDD "*Forma de iniciación del procedimiento y duración*" en su apartado 2 dispone:

"(…)
2. Cuando el procedimiento tenga por objeto la determinación de la posible existencia de una infracción de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, se iniciará mediante acuerdo de inicio adoptado por propia iniciativa o como consecuencia de reclamación.
(…)

Cuando fuesen de aplicación las normas establecidas en el artículo 60 del Reglamento (UE) 2016/679, el procedimiento se iniciará mediante la adopción del proyecto de acuerdo de inicio de procedimiento sancionador, del que se dará conocimiento formal al interesado a los efectos previstos en el artículo 75 de esta ley orgánica."

Y el artículo 75 "*Interrupción de la prescripción de la infracción"* de la LOPDGDD establece:

"(…)
Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679 interrumpirá la prescripción el conocimiento formal por el interesado del proyecto de acuerdo de inicio que sea sometido a las autoridades de control interesadas".

Y la Disposición adicional cuarta "*Suspensión de plazos de prescripción y caducidad*" del Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 dispuso que:

"Los plazos de prescripción y caducidad de cualesquiera acciones y derechos quedarán suspendidos durante el plazo de vigencia del estado de alarma y, en su caso, de las prórrogas que se adoptaren."

Y el artículo 9 "P*lazos administrativos suspendidos en virtud del Real Decreto 463/2020, de 14 de marzo.*" del Real Decreto 537/2020, de 22 de mayo, por el que se prorroga el estado de alarma declarado por el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 estableció que:

"Con efectos desde el 1 de junio de 2020, el cómputo de los plazos administrativos que hubieran sido suspendidos se reanudará, o se reiniciará, si así se hubiera previsto en una norma con rango de ley aprobada durante la vigencia del estado de alarma y sus prórrogas."

En el presente caso, se trata de un procedimiento sancionador en el que la AEPD ostenta la condición de autoridad de control principal, por tratarse de un tratamiento transfronterizo que realiza una empresa (la parte recurrente) que tiene su establecimiento principal en España y presta servicios a varios países de la Unión Europea, por lo que resulta de aplicación las normas establecidas en el artículo 60 del RGPD. Por tanto, es la adopción del proyecto de acuerdo de inicio de procedimiento sancionador el que da inicio al procedimiento sancionador e interrumpe la prescripción de la infracción el conocimiento formal del proyecto de acuerdo de inicio por parte de la parte recurrente.

Según consta en el expediente, el proyecto de acuerdo de inicio del presente procedimiento sancionador se adoptó el 18 de mayo de 2022 y fue notificado a la parte recurrente el 27 de mayo de 2022.

Por tanto, siendo el *dies ad quem* del plazo de prescripción de dos años el 18 de mayo de 2022, pero teniendo en cuenta que debido a la situación excepcional a que dio lugar el COVID-19 se suspendieron tanto los plazos de prescripción como de caducidad desde el 14 de marzo de 2020 hasta el 1 de junio de 2020, la infracción de los artículos 25 y 32 del RGPD no estaba prescrita.

En especial, esta Agencia desea resaltar que el *dies ad quem* del plazo de prescripción de dos años por la infracción de los artículos 25 y 32 el RGPD, teniendo en cuenta la citada suspensión, sería el 8 de agosto de 2022.

Dado que el proyecto de acuerdo de inicio del procedimiento sancionador fue notificado a la parte recurrente el 27 de mayo de 2022, tal infracción no estaba prescrita.

Por todo lo expuesto, se desestima la presente alegación.

CUARTO-. DESPROPORCIONALIDAD DEL IMPORTE DE LA SANCIÓN. INEXISTENCIA DE LAS CIRCUNSTANCIAS AGRAVANTES ADUCIDAS Y EXISTENCIA DE CIRCUNSTANCIAS ATENUANTES NO TOMADAS EN CONSIDERACIÓN.

4.1. Cuestiones preliminares

En este apartado la parte recurrente se limita a realizar un resumen de la Resolución Sancionadora en lo referente a la graduación de la sanción por la infracción de los artículos 25 y 32 del RGPD, que considera no tuvo en cuenta las "*Directrices 4/2022 sobre el cálculo de las multas administrativas con arreglo al RGPD"*, adoptadas por el Comité Europeo de Protección de Datos el 12 de mayo de 2022 (en adelante, las "Directrices 4/2022").

Al respecto, esta Agencia señalar matizar que las citadas Directrices 4/2022 fueron sometidas a consulta pública, que finalizó el 27 de junio de 2022, y aún está pendiente su versión final.

4.2. La sanción impuesta vulnera el principio de proporcionalidad, ya que ha sido cuantificada contraviniendo los criterios establecidos en las Directrices 4/2022.

Alega la parte recurrente que el artículo 83.1 del RGPD prevé que las multas administrativas que impongan las autoridades de control serán, en cada caso individual, efectivas, proporcionadas y disuasorias. Por tanto, indiscutiblemente uno de los principios que rigen en todo procedimiento sancionador en materia de protección de datos es el principio de proporcionalidad.

Indica que este principio de proporcionalidad es propio de cualquier procedimiento sancionador, constituye el principio fundamental que preside el proceso de graduación de las sanciones e implica su adecuación a la gravedad del hecho constitutivo de la infracción, como así lo exige el artículo 29.3 de la LRJSP.

Explica la parte recurrente que toda sanción debe determinarse en congruencia con la entidad de la infracción cometida y según un criterio de proporcionalidad en relación

con las circunstancias del hecho. Y cita el Tribunal Supremo en sus Sentencias núm. 6602/2004, de 3 de diciembre y núm. 5149/2009, de 12 de abril.

Alega la parte recurrente que en aras de garantizar una aplicación uniforme del régimen sancionador previsto en el artículo 83.1 del RGPD, y que garantice el principio de proporcionalidad, el Comité Europeo de Protección de Datos adoptó las Directrices 4/2022, las cuales establecen una clara metodología para calcular las sanciones.

Y que de acuerdo con lo previsto en el párrafo número 61 de las Directrices 4/2022, se debería calcular un importe inicial de la sanción a través de un rango de porcentajes, los cuales dependen de la gravedad de la infracción imputada. En el caso de las infracciones con una gravedad media, equiparables a las sanciones graves previstas en el artículo 73 de la LOPDGDD, entiende que el importe inicial debería fijarse en un rango de entre el 10 y el 20% del máximo legal aplicable.

Explica la parte recurrente que el máximo legal aplicable sería del 2% del volumen anual de negocios, el cual se ha determinado en ******CANTIDAD.1***. Y que, por tanto, el importe inicial se debería fijar en una horquilla de entre el 0,2% del volumen anual de negocios (******CANTIDAD.2***) y el 0,4% del volumen anual de negocios (******CANTIDAD.3***). Por lo que la sanción impuesta por la Resolución Sancionadora, con un importe de 550.000 euros, ya habría sobrepasado el límite máximo de esta horquilla.

Al respecto, esta Agencia desea señalar que una cuestión es la tipificación de una infracción según el RGPD y otra muy distinta es la clasificación de dicha infracción a efectos de prescripción conforme la LOPDGDD.

Las infracciones en materia de protección de datos están tipificadas en los apartados 4, 5 y 6 del artículo 83 del RGPD. Es una tipificación por remisión, admitida plenamente por nuestro Tribunal Constitucional. En este sentido, también el artículo 71 de la LOPDGDD realiza una referencia a las mismas al señalar que "*Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica*".

En este sentido, el Dictamen del Consejo de Estado de 26 de octubre de 2017 relativo al Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal dispone que "*El Reglamento Europeo sí tipifica, por más que lo haga en un sentido genérico, las conductas constitutivas de infracción: en efecto, los apartados 4, 5 y 6 de su artículo 83 arriba transcritos contienen un catálogo de infracciones por vulneración de los preceptos de la norma europea que en tales apartados se indican. El artículo 72 del Anteproyecto asume, no en vano, la existencia de dicho catálogo, cuando dispone que "constituyen infracciones los actos y conductas que supongan una vulneración del contenido de los apartados 4, 5 y 6 del Reglamento Europeo y de la presente ley orgánica".*

Por su parte, las infracciones fijadas en los artículos 72, 73 y 74 de la LOPDGDD lo son sólo a los efectos de la prescripción, tal y como reza el inicio de todos y cada uno de estos preceptos. Esta necesidad surgió en nuestro Estado dado que no existe en el

RGPD referencia alguna a la prescripción relativa a las infracciones, ya que este instituto jurídico no es propio de todos los Estados miembros de la UE.

Debe partirse de que el RGPD es una norma jurídica directamente aplicable, que ha sido desarrollada por la LOPDGDD, sólo en aquello que le permite el primero. Así queda patente y en cuanto a la prescripción en la propia exposición de motivos de la LOPDGDD cuando expresa que *"La categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, teniendo la descripción de las conductas típicas como único objeto la enumeración de manera ejemplificativa de algunos de los actos sancionables que deben entenderse incluidos dentro de los tipos generales establecidos en la norma europea. La ley orgánica regula los supuestos de interrupción de la prescripción partiendo de la exigencia constitucional del conocimiento de los hechos que se imputan a la persona".*

Resulta de la aplicación e interpretación del RGPD, y no de la LOPDGDD, el que determina la gravedad de una infracción atendiendo a una serie de condicionantes previstos en el mismo.

Como se puede comprobar, no está presente en el RGPD una tipificación en infracciones muy graves, graves o leves típica del ordenamiento jurídico español, ni tampoco puede deducirse de su dicción que la vulneración de los preceptos del artículo 83.4 del RGPD correspondan a infracciones leves y los preceptos del artículo 83.5 o del artículo 83.6 del RGPD correspondan a infracciones graves.

Así, el considerando 148 habla de infracciones graves en contraposición con las leves cuando determina que *"En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante.".*

Por todo ello, la gravedad de una infracción se determina a los efectos del RGPD y con los elementos dotados por éste.

De nuevo debe traerse a colación el Dictamen del Consejo de Estado precitado, que lo explica con verdadera profusión: *"Por otra parte, el Reglamento Europeo no distingue, al fijar la cuantía de las sanciones, entre infracciones muy graves, graves y leves, como dice la exposición de motivos del Anteproyecto. En realidad, la norma europea se limita a distinguir, en función del límite cuantitativo máximo de la multa a imponer, entre unas infracciones que pueden ser sancionadas "con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior" (apartado 4 del artículo 83), y otras infracciones que pueden ser sancionadas "con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior"*

(apartados 5 y 6 del artículo 83). De esta distinción se colige que, para el Derecho de la Unión Europea, las infracciones tipificadas en los apartados 5 y 6 del artículo 83 pueden llegar a revestir una misma y mayor gravedad que las contempladas en el apartado 4 del mismo artículo 83 del Reglamento Europeo. La norma europea se limita pues a establecer dos categorías de infracciones en razón de su gravedad.

El Anteproyecto contempla, en cambio, tres categorías de infracciones: el artículo 73 del Anteproyecto considera infracciones "muy graves" la "vulneración sustancial" de los preceptos mencionados en los apartados 5 y 6 del artículo 83 del Reglamento Europeo; el artículo 74 del Anteproyecto considera infracciones "graves" la "vulneración sustancial" de los preceptos mencionados en el apartado 4 del artículo 83 del Reglamento Europeo; y el artículo 75 considera infracciones "leves" las restantes "infracciones de carácter meramente formal" de los preceptos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento Europeo.

La tripartición realizada por el Anteproyecto resulta de la distinción entre "vulneraciones sustanciales" e "infracciones meramente formales" de los preceptos mencionados en el apartado 4, 5 y 6 del artículo 83 del Reglamento Europeo: si se trata de vulneraciones sustanciales, serán consideradas infracciones "muy graves", cuando los preceptos vulnerados sean los mencionados en los apartados 5 y 6, o "graves", cuando los preceptos vulnerados sean los mencionados en el apartado 4, mientras que si se trata de infracciones meramente formales de tales preceptos, serán consideradas en todo caso como "leves".

Esta distinción entre "vulneraciones sustanciales" e "infracciones meramente formales" y la consiguiente inclusión de una tercera categoría de "infracciones leves", distinta de las infracciones graves y muy graves, se ha realizado -como resulta del expediente y del propio tenor del Anteproyecto- a los solos efectos del establecimiento de los plazos de prescripción de las infracciones y no de la determinación de la cuantía de las multas administrativas, lo que exige, para su mejor comprensión, algunas aclaraciones adicionales.

Los plazos de prescripción de las infracciones no se encuentran previstos en el Reglamento Europeo y, por tanto, existe el entendimiento, tácito pero pacífico, de que los Estados miembros ostenta competencia para el establecimiento de tales plazos. La determinación de tales plazos debe estar en función, como es bien conocido, de la gravedad de la infracción. Pues bien, las infracciones previstas apartado 4 del artículo 83, de una parte, y en los apartados 5 y 6 del artículo 83 del Reglamento Europeo, de otra, tienen un diferente límite máximo -10.00.000 euros o el 2% del volumen de negocio en el primer caso, 20.000.000 euros o el 4% del volumen de negocio en el segundo- pero el mismo límite mínimo, que en ambos casos es de 1 euro. La existencia de tan amplios márgenes cuantitativos indica que las infracciones del artículo 83, sean las del apartado 4 sean las de los apartados 5 y 6, puede ser de muy diferente entidad y que, por tal razón, no pueden tener el mismo plazo de prescripción aquellas infracciones que, por su gravedad, se encuentren próximas al límite cuantitativo superior que aquellas otras que, por su levedad, estén más cerca del límite cuantitativo inferior. En tales circunstancias, la fijación de los plazos de prescripción no quedaría resuelta de forma satisfactoria aplicando a las infracciones de los preceptos mencionados en los apartados 5 y 6 del artículo 83 un plazo superior que a las infracciones de los preceptos mencionados en el apartado 4 del artículo 83,

dado que las infracciones contempladas unos y otros preceptos, en caso de ser leves, exigirían un plazo de prescripción inferior.

Desde este punto de vista y con el único objeto de establecer su plazo de prescripción, el Anteproyecto ha distinguido entre "infracciones meramente formales" y "vulneraciones sustanciales" de tales preceptos, considerando a las primeras como "infracciones leves" con un plazo de prescripción de un año y a las segundas como "infracciones graves" y "muy graves" con unos plazos de prescripción de dos y tres años respectivamente. A juicio del Consejo de Estado, esta clasificación de las infracciones, en la medida en que se realiza a los solo efectos de determinar unos plazos de prescripción de las infracciones no previstos en el Reglamento Europeo, no puede entenderse contraria a lo dispuesto en la norma europea.

Esta clasificación no tiene, sin embargo, trascendencia en cuanto al importe de las multas. La determinación de la cuantía de las multas a imponer por la vulneración de los preceptos mencionados en los apartados 4, 5 y 6 del artículo 83 del Reglamento Europeo compete, de acuerdo con la norma europea, a las autoridades de control, de acuerdo con los criterios de graduación establecidos en el apartado 2 de este mismo precepto, entre los que se encuentra la "naturaleza" o "gravedad" de la infracción". Dentro de los límites cuantitativos establecidos por el Reglamento Europeo, las autoridades de control, atendiendo a la mayor o menor gravedad de la infracción, deben fijar el importe de las multas. Ciertamente, los márgenes con que cuentan las autoridades de control son amplísimos -de 1 euro a 10.000.000 euros por infracción de los preceptos mencionados en el apartado 4 del artículo 83 y de 1 euro a 20.000.000 euros por infracción de los preceptos mencionados en los apartados 5 y 6-, lo que confiere a tales autoridades un elevado grado de discrecionalidad, muy superior a los que suele ser habitual en países de nuestra tradición jurídica. Se trata, en todo caso, del modelo querido por el Reglamento Europeo, de ahí que la distinción entre infracciones leves, graves y muy graves contemplada en el Anteproyecto no pueda tener consecuencia en la determinación de la cuantía máxima de las infracciones leves, debiendo estarse en todo caso a la determinación de su importe que hagan las autoridades de control, conforme a las circunstancias del caso concreto, dentro de los límites marcados en aquel reglamento".

Así, la clasificación de las infracciones a los efectos de la prescripción de la LOPDGDD no tiene virtualidad en cuanto a la determinación de la gravedad de la infracción a los efectos del RGPD ni respecto de la imposición de las multas correspondientes, en su caso.

A título meramente ilustrativo se puede indicar que, una misma conducta, como por ejemplo la falta información en la política de privacidad de una empresa, pueda ser considerada grave o leve a los efectos del Reglamento (en atención a las circunstancias citadas en el considerando 148 en relación con las previsiones del artículo 83 del RGPD, pues no es lo mismo el incumplimiento por una empresa multinacional que por un autónomo) y en ambos casos con prescripción leve. La gravedad de una infracción determinará su sanción.

Por su parte, las citadas "*Directrices 04/2022 para el cálculo de las multas administrativas en virtud del RGPD*", en su apartado 4, párrafos 47 a 70, explican una

serie de criterios para fijar el punto de partida del cálculo armonizado de las multas a aplicarse.

En este sentido, el CEPD considera que tres elementos constituyen el punto de partida para este cálculo: la clasificación de las infracciones según su naturaleza con arreglo a los artículos 83 (4) a (6) del RGPD, la gravedad de la infracción con arreglo al artículo 83, apartado 2, del RGPD y el volumen de negocios de la empresa.

Respecto a la clasificación de las infracciones por su naturaleza, de acuerdo con el artículo 83.4.a) del RGPD, la infracción de las obligaciones del responsable y del encargado a tenor de los artículos 25 a 39 del RGPD se sancionarán con multas administrativas de 10.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

En el presente caso, se considera un hecho probado que la parte recurrente ha tenido un volumen de negocio de ******CANTIDAD.1*** en el año 2021.

Por tanto, el máximo de multa aplicable sería un 2% de este monto, es decir, ******CANTIDAD.4***.

Respecto a la gravedad de la infracción de acuerdo con el artículo 83.2 del RGPD, las citadas Directrices 04/2022 indican que el RGPD establece que debe prestarse la debida atención a las circunstancias que califican la gravedad de la infracción en un caso individual. Y que el RGPD exige a la autoridad de control que preste la debida atención a la naturaleza, la gravedad y la duración de la infracción, teniendo en cuenta la naturaleza, el alcance o la finalidad del tratamiento de que se trate, así como el número de interesados afectados y el nivel del perjuicio sufrido por ellos [artículo 83, apartado 2, letra a), del RGPD]; el carácter intencionado o negligente de la infracción [artículo 83, apartado 2, letra b), del RGPD]; y las categorías de datos personales afectadas por la infracción [artículo 83, apartado 2, letra g), del RGPD].

Y que la autoridad de control debe revisar estos elementos a la luz de las circunstancias del caso concreto y, sobre la base de este análisis, debe llegar a una conclusión sobre el grado de gravedad indicado en el apartado 61.

Para valorar la naturaleza, gravedad y duración de la infracción, las citadas Directrices indican que debe evaluarse los siguientes elementos específicos:

a) La naturaleza de la infracción: debe revisarse el interés que la disposición infringida pretende proteger y el lugar de la disposición infringida en el marco de la protección de datos. En el presente caso, los artículos 25 y 32 del RGPD pretenden proteger la seguridad y la confidencialidad de los datos, así como garantizar un enfoque de protección de datos antes y durante todo el tratamiento, que asegure el cumplimiento de los requisitos del RGPD y proteger los derechos de los interesados. Además, las Directrices disponen que la autoridad de control podrá examinar en qué medida la infracción prohibía la aplicación efectiva de la disposición y el cumplimiento del objetivo que pretendía proteger. En el presente caso, la infracción en cuestión

impidió el objetivo perseguido por las disposiciones infringidas, toda vez que se vio vulnerada la seguridad de los datos personales de los repartidores y se vieron vulnerados sus derechos.

b) La gravedad de la infracción, evaluada en función de las circunstancias específicas:

i. La naturaleza del tratamiento, incluido el contexto en el que se basa funcionalmente y todas las características del tratamiento. Las citadas Directrices disponen que cuando la naturaleza del tratamiento entrañe mayores riesgos, por ejemplo, cuando se tomen decisiones o medidas con efectos negativos para los interesados, como en el presente caso, en que la utilización del “excellence score” podía determinar que un determinado repartidor se quedara fuera de una determinada franja horaria, con el correspondiente detrimento en sus ingresos, la autoridad de control podrá considerar conceder más peso a este factor. También disponen las citadas Directrices que una autoridad de control puede conceder más peso a este factor cuando exista un claro desequilibrio entre los interesados y el responsable del tratamiento (por ejemplo, cuando los interesados sean empleados del responsable de tratamiento, como en el presente caso).

ii. El alcance del tratamiento, con referencia al alcance local, nacional o transfronterizo del tratamiento llevado a cabo y la relación entre esta información y el alcance real del tratamiento en términos de asignación de recursos por parte del responsable del tratamiento. Las citadas Directrices explican que este elemento pone de relieve un factor de riesgo real, vinculado a la mayor dificultad del interesado y de la autoridad de control para frenar las conductas ilícitas a medida que aumenta el alcance del tratamiento. Cuanto mayor sea el alcance del tratamiento, mayor será el peso que la autoridad de control pueda atribuir a este factor. En el presente caso, se trata de un tratamiento transfronterizo realizado a todos los datos que disponía la parte recurrente de todos sus repartidores que trabajaban en la Unión Europea, por lo que el alcance del tratamiento era considerablemente amplio.

iii. La finalidad del tratamiento**:** Las citadas Directrices explican que la autoridad de control también puede considerar si la finalidad entra dentro de las denominadas actividades básicas del responsable del tratamiento. Y que cuanto más central sea el tratamiento en las actividades principales del responsable o del encargado del tratamiento, más graves serán las irregularidades en este tratamiento. La autoridad de control podrá conceder más peso a este factor en estas circunstancias. En el presente caso, el tratamiento de los datos personales de sus repartidores en base al “excellence score” era un tratamiento central entre las actividades realizadas de la parte recurrente.

iv. El número de interesados concretamente, pero también potencialmente afectados: Las citadas Directrices indican que cuanto mayor sea el número de interesados implicados, mayor será el peso que la autoridad de control pueda atribuir a este factor. Y que en muchos casos, también puede considerarse que la infracción adquiere connotaciones «sistémicas» y, por lo tanto, puede afectar, incluso en momentos diferentes, a otros interesados que no hayan presentado reclamaciones o informes a la autoridad de control. Y que dependiendo de las circunstancias del caso, la autoridad de control podrá considerar la relación entre el número de interesados afectados y el número total de interesados en ese contexto (por ejemplo, el número de ciudadanos, clientes o empleados), a fin de evaluar si la infracción es de carácter sistémico. En el presente caso, se consideró afectados los derechos de 7073 repartidores de la parte recurrente, esto es, la totalidad de sus repartidores en activo en un mes determinado, por lo que se considera que la infracción en cuestión adquirió connotaciones “sistémicas” al decir de las citadas Directrices.

v. El nivel del perjuicio sufrido y la medida en que el comportamiento puede afectar a los derechos y libertades individuales: las citadas Directrices indican que, de conformidad con el considerando 75 del RGPD, el nivel de los daños sufridos se refiere a los daños físicos, materiales o inmateriales. En el presente caso, ha quedado acreditado que se vio vulnerada la intimidad de todos los repartidores de Glovo que trabajaban en la Unión Europea.

a) La duración de la infracción**:** las citadas Directrices disponen que, en general, una autoridad de control puede atribuir más peso a una infracción de mayor duración. Y señalan que una determinada conducta podría haber sido ilícita también en el marco regulador anterior, añadiendo así un elemento adicional para evaluar la gravedad de la infracción. Y que cuanto mayor sea la duración de la infracción, mayor será el peso que la autoridad de control pueda atribuir a este factor. En el presente caso, ha quedado acreditado que la infracción ha tenido lugar desde la fundación de Glovo en 2014 hasta mayo de 2020.

En cuanto al carácter intencional o negligente de la infracción, en el presente caso esta Agencia ya ha indicado en numerosas ocasiones que no considera que hubiera existido voluntad de infringir por parte de la parte recurrente, sino que considera que ésta ha actuado de forma gravemente negligente. Al respecto, las citadas Directrices indican que, en función de las circunstancias del caso, la autoridad de control también podrá ponderar el grado de negligencia. La parte recurrente es una gran empresa en su sector de negocio, que debe velar por los derechos y libertades de sus trabajadores, entre otros, el derecho fundamental a la protección de sus datos personales. En el presente caso, esta Agencia considera que no ha sido diligente a la hora de configurar su sistema de permisos. En especial, teniendo en cuenta que se trata no solo de una gran empresa de la que cabría exigir una mayor profesionalidad,

sino que es una entidad habituada al tratamiento de datos personales. En este sentido, resulta muy ilustrativa, la SAN de 17 de octubre de 2007 (rec. 63/2006), la cual indica que *"…el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto".*

Negar la concurrencia de una actuación negligente por parte de la parte recurrente equivaldría a reconocer que su conducta -por acción u omisión- ha sido diligente. Obviamente, no se comparte esta perspectiva de los hechos, puesto que ha quedado acreditada la falta de diligencia debida.

Esta Agencia se reitera en que a lo largo del correspondiente procedimiento sancionador ha quedado acreditado que el sistema de permisos de acceso a los datos de los repartidores, instaurado por la parte recurrente, no cumplía en un primer momento con los principios y obligaciones que establece el RGPD, toda vez que la empresa no realizó un análisis previo al tratamiento en el que se analizaran debidamente las posibles implicaciones para los derechos y libertades de los interesados y se determinaran en base al mismo las medidas adecuadas al sistema de gestión de permisos de acceso. Más bien al contrario, la parte recurrente no adoptó una postura proactiva sino más bien una actitud reactiva, modificando la gestión de los permisos de acceso a los datos personales de los repartidores como si se tratara de "parches" informáticos, solucionando los problemas a medida que se los iban encontrando conforme cambiaba la estructura de la organización, tal y como ha sido expuesto en sus alegaciones durante el procedimiento sancionador.

Por la importancia del bien jurídico protegido, la parte recurrente estaba obligada a encontrar soluciones de organización que no supusieran un mayor riesgo para los derechos y libertades de sus repartidores y que garantizaran la seguridad de los datos, sin importar el tamaño de su organización ni el número de empleados con que contaba, dado que estos riesgos eran los que debían tenerse en cuenta sin importar el número de repartidores en un momento determinado.

El sistema de permisos de acceso a los datos de los repartidores no se configuró en los momentos iniciales teniendo en cuenta los posibles riesgos para los derechos y libertades de sus repartidores ni se configuró de modo que, por defecto, no resultaran accesibles los datos de los repartidores si no era necesario para la finalidad. La parte recurrente debió asegurarse de que, por defecto, el acceso a los datos de los repartidores estuviera limitado al ámbito geográfico necesario, en cumplimiento del artículo 25.2 del RGPD.

Sentado lo anterior, puede afirmarse que, de la instrucción del procedimiento, se constató también, entre otros, la falta de un mecanismo de permisos de acceso a los datos personales de los repartidores que impidiera el acceso de los usuarios a datos que no eran necesarios y que garantizara la seguridad de los datos, como exige el art. 32 del RGPD.

Igualmente, el hecho de que la parte recurrente hubiera implementado posteriormente modificaciones en las medidas técnicas u organizativas existentes, corrobora que aquellas otras no proporcionaban la seguridad adecuada.

Por todo lo expuesto, esta Agencia considera que el comportamiento de la parte recurrente ha sido gravemente negligente.

En cuanto a las categorías de datos personales afectadas por la infracción, las citadas Directrices explican que el RGPD destaca claramente los tipos de datos que merecen una protección especial y, por tanto, una respuesta más estricta en términos de multas, haciendo especial referencia a los datos fuera del ámbito de aplicación de los artículos 9 y 10 del RGPD cuya difusión cause daños o dificultades inmediatos al interesado, como por ejemplo, datos de localización, como en el presente caso.

Una vez evaluados todos los aspectos anteriores, las citadas Directrices disponen que todos ellos determinan la gravedad de la infracción en su conjunto. Y que sobre la base de la evaluación de los factores descritos anteriormente, la autoridad de control podrá considerar que la infracción es de un nivel bajo, medio o alto de gravedad, sin perjuicio de la cuestión de si puede o no imponerse una multa.

En el presente caso, en virtud de todo el análisis anteriormente expuesto, esta Agencia considera que la infracción en cuestión es de un nivel alto de gravedad.

Al respecto, las citadas Directrices indican que al calcular las infracciones de elevado nivel de gravedad de las multas administrativas, la autoridad de control determinará el importe de partida para el cálculo ulterior en un punto comprendido entre el 20 y el 100 % del máximo legal aplicable.

Por tanto, en el presente caso, el importe de partida para el cálculo de la multa estaría comprendido entre el 20% y el 100% de ******CANTIDAD.4***, es decir, entre ******CANTIDAD.3*** y ******CANTIDAD.4***.

En segundo lugar, alega la parte recurrente que el párrafo 67 de las Directrices 4/2022 prevé que en las compañías con un volumen de negocios de entre 100 millones hasta 250 millones, los cálculos iniciales anteriores se llevarán a cabo sobre la base de un importe inferior al 20% del importe inicial identificado. Y que, por tanto, la horquilla anterior debería rebajarse en un 20%, de manera que el rango estaría entre los ******CANTIDAD.5*** y los ******CANTIDAD.6***.

Entiende la parte recurrente que la sanción impuesta superaría esta horquilla máxima que se debe aplicar teniendo en cuenta el importe del volumen de negocios de GLOVO.

En cuanto al volumen de negocios de la empresa, las citadas Directrices permite que la autoridad de control ajuste el importe de partida correspondiente a la gravedad de la infracción en los casos en que dicha infracción sea cometida por una empresa cuyo volumen de negocios anual no exceda de 100 millones de euros, cuyo volumen de negocios anual no exceda de 250 millones de euros y un volumen de negocios anual no superior a 500 millones de euros. En el caso de las empresas con un volumen de negocios anual de 100 millones EUR hasta 250 millones EUR, permite a las

autoridades de supervisión considerar la posibilidad de efectuar cálculos sobre la base de un importe que minore un 20 % el importe de partida identificado.

En el presente caso, se podría considerar que el importe de partida para imponer una multa administrativa debería fijarse entre ******CANTIDAD.6*** y ******CANTIDAD.5***. No obstante, cabe destacar que las citadas Directrices hacen hincapié en que estas cifras son los puntos de partida para el cálculo posterior, y no los importes fijos para las infracciones de las disposiciones del RGPD. Y que la autoridad de control tiene la facultad discrecional de utilizar la totalidad de las multas, desde cualquier multa mínima hasta el máximo legal, garantizando que la multa se adapte a las circunstancias del caso.

Como puede observarse, la multa impuesta por esta Agencia de 550.000€ no supera (ni tan siquiera se acerca) al máximo que se debería aplicar teniendo en cuenta el importe del volumen de negocios de la parte recurrente.

Por todo lo expuesto, se desestima la presente alegación.

4.3. Inexistencia de las circunstancias agravantes alegadas por la AEPD en su Resolución Sancionadora

Alega la parte recurrente que la Resolución Sancionadora considera que concurrirían 3 circunstancias agravantes que modularían la sanción impuesta, pero que ninguna de estas agravantes concurre en este caso, de acuerdo con los siguientes motivos:

I. Naturaleza gravedad y duración de la infracción —apartado a) del artículo 83.2 del RGPD—:

En la Resolución Sancionadora se justifica que concurre esta agravante por la afectación a los derechos de 7.073 repartidores. No obstante, alega la parte recurrente que no se ha acreditado que la presunta infracción causara daños alguno cuantificable para los interesados, de manera que no cabe afirmar que se haya producido una afectación al bien jurídico protegido por esta agravante.

Alega la parte recurrente que la Resolución Sancionadora se limita a indicar que "*el nivel de daños sufrido por los interesados es uno de los posibles criterios de graduación*" (véase página 117), pero que pueden existir otros criterios para apreciar esta agravante. Sin embargo, entiende la parte recurrente que no se especifica ni se motiva por qué aprecia la concurrencia de esta agravante cuando precisamente no se han causado daños.

Por ello, entiende la parte recurrente que no debe apreciarse esta agravante, ya que la Resolución Sancionadora no justifica por qué motivo debe aplicarse esta agravante, cuando ha quedado acreditado que la supuesta infracción no ha causado daño alguno a los interesados.

Al respecto, esta Agencia desea recordar el literal de la Resolución Sancionadora sobre esta cuestión:

"(…) Como agravantes:

- La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido (apartado a): por la afectación a los derechos de 7073 trabajadores (número de repartidores activos en España durante los últimos 30 días que consta en el Informe de Actuaciones Previas de la investigación que dio lugar al presente procedimiento sancionador), hasta que se corrigió el sistema de permisos, al menos, hasta el 18 de mayo de 2020.
(…)"

Es decir, el apartado a) del artículo 83.2 del RGPD establece que debe analizarse la naturaleza, gravedad y duración de la infracción. Y que para ello debe tenerse en cuenta:
- la naturaleza, alcance o propósito de la operación de tratamiento de que se trate
- así como el número de afectados
- y el nivel de los daños y perjuicios que hayan sufrido

En ningún momento dice el citado artículo del RGPD que estas tres cuestiones sean las únicas que deban tenerse en cuenta para analizar la naturaleza, gravedad y duración de la infracción.

Y mucho menos dice que uno solo de estos aspectos, como es el nivel de los daños y perjuicios sufridos, sea el único a tener en cuenta para los citados fines.

En este sentido, tal y como puede observarse y en cumplimiento de lo estipulado por el artículo 83.2.a) del RGPD, la Resolución Sancionadora en este apartado ha destacado el hecho de que la infracción ha afectado los derechos de 7073 repartidores y que esto fue así hasta el 18 de mayo de 2020. Todo ello a efectos de valorar la naturaleza, gravedad y duración de la infracción en cuestión.

Por lo demás, esta Agencia se reitera en lo ya expuesto en su análisis sobre el apartado a) del artículo 83.2 del RGPD, para realizar el cálculo de la multa máxima que cabría imponer.

Por todo lo expuesto, se desestima la presente alegación.

II. La forma en que la autoridad de control tuvo conocimiento de la infracción —apartado h) del artículo 83.2 del RGPD—:

Alega la parte recurrente que la Resolución Sancionadora considera que concurre esta agravante ya que "*se tuvo conocimiento a través de una petición de la autoridad italiana de protección de datos*".

Pero considera que este hecho, por sí mismo, no es suficiente para justificar la existencia de esta agravante.

Indica la parte recurrente que según lo dispuesto en el punto 98 de las Directrices 4/2022, el hecho de que se tenga conocimiento de la infracción a través de una denuncia o una investigación debe ser un hecho neutro.

Además, indica que según ese mismo punto de las Directrices 4/2022, esta circunstancia solamente se puede apreciar como una atenuante en el supuesto en que sea el propio infractor el que notifique, de *mutu propio*, la infracción cometida al margen de cualquier procedimiento de inspección o de obligación de notificación ordinaria.

Por tanto, alega la parte recurrente que no puede apreciarse esta agravante por el simple hecho que el procedimiento sancionador se haya incoado a raíz de una denuncia por parte de otra autoridad de protección de datos.

Al respecto, esta Agencia desea señalar que las citadas Directrices disponen que:

"De conformidad con el artículo 83, apartado 2, letra h), la forma en que la autoridad de control tuvo conocimiento de la infracción podría ser un factor agravante o atenuante pertinente. (…)

Cuando la autoridad de control haya tenido conocimiento de la infracción, por ejemplo, mediante una reclamación o una investigación, este elemento también debe considerarse, por regla general, neutro. La autoridad de control podrá considerar esta circunstancia atenuante si el responsable o el encargado del tratamiento notifican la infracción de oficio, antes de que la autoridad de control tenga conocimiento del caso". (el subrayado es de esta Agencia)

Es decir, las Directrices permiten que la autoridad de control valore la forma en que se hubiera tenido conocimiento de la infracción como un agravante, teniendo en cuenta las circunstancias del caso concreto. En cuanto a que si la autoridad de control hubiera tenido conocimiento de la infracción a través de una investigación esto deba ser considerado como un factor neutro, las mismas Directrices aclaran que ello es una regla general, por tanto, se contempla que pudiera existir excepciones en las que esto no fuera así.

En el presente caso, se trata de un caso muy particular, en el se vieron involucradas autoridades de varios Estados Miembros, que se originó porque la autoridad de control de uno de estos Estados llevó a cabo una amplia investigación sobre diversos aspectos del tratamiento que la parte recurrente realizaba sobre un colectivo tan expuesto como el de sus repartidores, considerados población vulnerable toda vez que existía un desequilibrio de poder en esa relación, dado que los repartidores no podían oponerse al tratamiento en cuestión si querían trabajar con la parte recurrente.

Por todo lo expuesto, se desestima la presente alegación.

III. Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso —apartado k) del artículo 83.2 del RGPD—:

Alega la parte recurrente que la Resolución Sancionadora considera que es un factor agravante, subsumible en el apartado k) del artículo 83.2 del RGPD, el hecho GLOVO sea "*una gran empresa en su sector de negocio*" de la que "*cabría exigir una mayor profesionalidad*".

Para ello se apoya en la Sentencia de la Audiencia Nacional, de 17 de octubre de 2007, dictada en el recurso 63/2006.

Entiende la parte recurrente que la aplicación de esta agravante es totalmente improcedente y resulta manifiestamente contraria a Derecho, ya que lo que se pretende es imponer una "sanción ejemplarizante" a GLOVO por ser quien es.

Alega la parte recurrente que el hecho de que GLOVO sea una gran empresa no puede conllevar, por sí mismo, un mayor reproche en la sanción de hechos presuntamente infractores. Lo único que puede significar es que no se pueda alegar un error de prohibición de derecho o una ausencia de culpabilidad, que es precisamente lo que se resolvió en la Sentencia de la Audiencia Nacional citada en la Resolución Sancionadora:

"*Así, en relación con el error de prohibición que se invoca en la demanda, debemos señalar que debido a la profesionalidad de la recurrente no puede invocarse el desconocimiento de una LO que desarrolla un derecho fundamental, cuando se desarrolla una actividad en constante contacto con datos personales, no puede invocarse, por tanto, con éxito error en la prohibición que, en todo caso, sería fácilmente vencible*". (el destacado es nuestro)

Por tanto, entiende la parte recurrente que la profesionalidad de GLOVO impediría apreciar que no ha actuado de manera culposa en la causación del hecho infractor, pero en modo alguno ello puede determinar la aplicación de una agravante.

Alega la parte recurrente que en el modo en que ha sido aplicada, esta agravante supone atribuir un mayor reproche punitivo a GLOVO por ser quien es, hecho que supone aplicar un derecho sancionador de autor incompatible con nuestro ordenamiento jurídico. Y que se instrumentaliza a GLOVO con una finalidad de prevención general, atribuyendo un mayor reproche jurídico a sus conductas de manera que el resto de empresas del sector se vean compelidas a actuar en un determinado sentido.

Cita la parte recurrente la Sentencia del Tribunal Constitucional núm. 150/1991, de 4 de julio, en la que se ha señalado que un derecho penal de autor, basado en el sujeto que comete la infracción y no en el hecho cometido, es incompatible con la Constitución.

Por tanto, entiende la parte recurrente que esta agravante debe ser rechazada frontal y rotundamente, ya que no cabe hacer un mayor reproche jurídico a GLOVO por ser una gran empresa, quien se sujeta al ordenamiento jurídico en igualdad de condiciones con el resto de operadores, sin que quepa exigirle "*una mayor diligencia*".

Al respecto, esta Agencia desea señalar que de ninguna manera se le impone "una "sanción ejemplarizante" a GLOVO por ser quien es".

De hecho, la multa impuesta está muy cercana al mínimo posible que proponen las citadas Directrices 04/2022, teniendo en cuenta la gravedad de la infracción, tal y como se ha explicado detalladamente en los apartados anteriores de esta resolución.

Por lo que difícilmente pueda entenderse que se trate de una sanción que pretenda dar ejemplo al resto de operadores.

En cuanto a la diligencia exigible a la parte recurrente, este aspecto ya ha sido analizado previamente, por lo que esta Agencia se limita a lo ya reseñado.

Por todo lo expuesto, se desestima la presente alegación.

4.4. Existencia de circunstancias atenuantes adicionales

Alega la parte recurrente que deberían aplicarse las circunstancias atenuantes adicionales siguientes:

I. La atenuante prevista en el artículo 83.2.e) del RGPD, ya que no existen incumplimientos previos:

Alega la parte recurrente que la falta de reincidencia o reiteración fue establecida como una "*atenuante de especial relevancia*" en la resolución sancionadora del procedimiento sancionador 120/2021, dirigido contra MERCADONA, S.A.

Y que en aplicación del principio de igualdad en la aplicación de la ley, esta misma atenuante debería ser aplicada a GLOVO, ya que GLOVO no ha sido sancionado con anterioridad por los hechos objeto de la Resolución Sancionadora.

Al respecto, esta Agencia desea señalar que el hecho de no haber sido sancionado con anterioridad solo puede operar como agravante y en ningún caso como atenuante.

En este sentido, la Audiencia Nacional en su SAN de 5 de mayo de 2021 (Rec. 1437/2020) sobre el apartado e) del artículo 83.2. del RGPD, respecto a la comisión de infracciones anteriores, ha manifestado que:

> "*Considera, por otro lado, que debe apreciarse como atenuante la no comisión de una infracción anterior. Pues bien, el artículo 83.2 del RGPD establece que debe tenerse en cuenta para la imposición de la multa administrativa, entre otras, la circunstancia "e) toda infracción anterior cometida por el responsable o el encargado del tratamiento". Se trata de una circunstancia agravante, el hecho de que no concurra el presupuesto para su aplicación conlleva que no pueda ser tomada en consideración, pero no implica ni permite, como pretende la actora, su aplicación como atenuante".*

Por todo lo expuesto se desestima la presente alegación.

II. La atenuante prevista en el artículo 83.2.k) del RGPD, por no haber obtenido ningún tipo de beneficios a través de la infracción.

Alega la parte recurrente que el hecho de no haber obtenido beneficio económico alguno a través de los hechos supuestamente infractores también debe ser considerada una atenuante, según lo previsto en el artículo 83.2.k) del RGPD.

Y que la existencia de esta atenuante cuando haya una ausencia de beneficios para el infractor ha sido apreciada por la Sentencia de la Audiencia Nacional, de 16 de diciembre de 2021, dictada en el recurso núm. 311/2018 (JUR 2022\65416).

Al respecto esta Agencia desea señalar que esta Sentencia de la Audiencia Nacional hace referencia al artículo 45.4 e) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la cual fue desplazada una vez resultó de aplicación el RGPD y derogada con la aprobación de la citada LOPDGDD.

Esta Agencia defiende que los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción sólo pueda ser considerado agravante y no un atenuante cuando no haya beneficios, de acuerdo con la citada Sentencia de la Audiencia Nacional, de 5 de mayo de 2021, rec. 1437/2020, que indica: "*Considera, por otro lado, que debe apreciarse como atenuante la no comisión de una infracción anterior". Pues bien, el artículo 83.2 del RGPD establece que debe tenerse en cuenta para la imposición de la multa administrativa, entre otras, la circunstancia "e) toda infracción anterior cometida por el responsable o el encargado del tratamiento". Se trata de una circunstancia agravante, el hecho de que no concurra el presupuesto para su aplicación conlleva que no pueda ser tomada en consideración, pero no implica ni permite, como pretende la actora, su aplicación como atenuante*". Aplicado al presente supuesto, la falta del presupuesto para su aplicación respecto del art. 76.2.c) de la LOPDGDD, esto es, obtener beneficios consecuencia de la infracción, no permite su aplicación como atenuante.

Este criterio de graduación se establece en la LOPDGDD de acuerdo con lo previsto en el artículo 83.2.k) del RGPD, según el cual las multas administrativas se impondrán teniendo en cuenta cualquier "factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción", entendiéndose que evitar una pérdida tiene la misma naturaleza a estos efectos que la obtención de beneficios.

Si a esto se añade que las sanciones deberán ser "en cada caso individual" efectivas, proporcionadas y disuasorias, conforme a lo previsto en el artículo 83.1 del RGPD, admitir la ausencia de beneficios como una atenuante, no solo es contrario a los presupuestos de hechos contemplados en el artículo 76.2.c), sino también contrario a lo establecido en el artículo 83.2.k) del RGPD y a los principios señalados.

Así, valorar la ausencia de beneficios como una atenuante anularía el efecto disuasorio de la multa, en la medida en que minora el efecto de las circunstancias que inciden efectivamente en su cuantificación, reportando al responsable un beneficio al que no se ha hecho merecedor. Sería una rebaja artificial de la sanción que puede llevar a entender que infringir la norma sin obtener beneficios, financieros o del tipo que fuere, no le producirá un efecto negativo proporcional a la gravedad del hecho infractor.

En todo caso, las multas administrativas establecidas en el RGPD, conforme a lo establecido en su artículo 83.2, se imponen en función de las circunstancias de cada caso individual y no se estima que la ausencia de beneficios sea un factor de graduación adecuado y determinante para valorar la gravedad de la conducta infractora. Solo en el caso de que esta ausencia de beneficios sea relevante para determinar el grado de antijuricidad y de culpabilidad presentes en la concreta actuación infractora podrá considerarse como una atenuante, en aplicación del artículo 83.2.k) del RGPD, que se re-

fiere a “cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso”.

Este párrafo deja una puerta abierta a aquellos supuestos en que la ausencia de beneficios pueda ser considerado circunstancia atenuante, mas no a tenor de la interpretación literal y teleológica del legislador conforme a la previsión del art. 83.2.k) del RGPD.

Por todo lo expuesto, se desestima la presente alegación.

Por último, alega la parte recurrente que, teniendo en cuenta la existencia de estas atenuantes y la ausencia de agravantes, según se ha acreditado, en el apartado anterior, como máximo la multa debería fijarse en el importe mínimo de la horquilla antes fijada; esto es, en ******CANTIDAD.5***.

Al respecto, esta Agencia señala que, dado que se desestimaron todas las alegaciones previas en este sentido, se desestima también la presente alegación. En cualquier caso, cabe destacar que el importe fijado como multa en la Resolución Sancionadora objeto del presente recurso se encuentra entre los valores mínimos posibles a imponer, de acuerdo con las indicaciones de las citadas Directrices 04/2022.

4.5. La existencia de circunstancias atenuantes adicionales justifica la reducción de la infracción

Alega la parte recurrente que, sin perjuicio de lo anterior, se debe tener en cuenta que, en aplicación del párrafo 140 de las Directrices 04/2022, el principio de proporcionalidad exige reducir esta cuantía cuando exista una imposibilidad de pago derivada de circunstancias excepcionales.

Y que concurren en este caso las circunstancias excepcionales a las que aluden las Directrices 04/2022, puesto que la crisis económica generada por la pandemia, que se extendió durante los años 2020 a 2022, así como el conflicto geopolítico entre Ucrania y Rusia desde 2022 han tenido, y seguirán teniendo, un gran impacto negativo en la economía de la compañía.

Alega la parte recurrente que la Cuenta de Pérdidas y Ganancias de ambos años 2021 y 2022 indican que GLOVO tuvo un resultado negativo de explotación en el año 2021 ***(…)***, y en el año 2022 ***(…)***, cifras que acreditan la delicada situación financiera en la que se encuentra la empresa y que su continuidad financiera depende en gran medida de su reputación y, consecuentemente, del resultado de procedimientos sancionadores como el presente.

Añade la parte recurrente que, como se acredita en el DOCUMENTO 2, en el pasado mes de febrero de 2023 Glovo no ha tenido más remedio ***(…)*** para tratar de paliar las severas pérdidas que ha ido teniendo debido a la coyuntura económica. Asimismo, se adjunta como DOCUMENTO 3 ***(…)***.

Por ello, alega la parte recurrente que estaría justificada que la sanción máxima de ******CANTIDAD.5*** fuera reducida en un grado, de manera que la sanción fuera de máximo ******CANTIDAD.7***.

Al respecto, esta Agencia desea reiterar lo ya expuesto en la citada Resolución Sancionadora objeto del presente recurso.

El artículo 83.4 del RGPD establece que:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:
a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"

Es decir, el RGPD no realiza ninguna mención a que deba considerarse si la empresa en cuestión está en una fase de expansión, o si la empresa tuvo un resultado negativo en su Cuenta de Pérdidas y Ganancias, ni la posible crisis de reputación que pudiera significar la imposición de dicha sanción, ni si existieron factores externos que pudieran afectar el negocio de la empresa en cuestión (tales como la pandemia del Covid-19 o la guerra en Ucrania), ***(…)***.

En este sentido, de la información que obra en Axesor ha quedado acreditado que GLOVOAPP ha facturado en 2021 un total de ******CANTIDAD.1***, por lo que la sanción de 550.000€ de multa que se había propuesto imponer no llega al 0,5% de dicho volumen, lo cual representaría la cuarta parte del máximo posible y estaría dentro de los valores mínimos posibles a imponer, de acuerdo con las indicaciones de las citadas Directrices 04/2022.

Por tanto, se desestima la presente alegación.

4.6. Importe sancionador correcto.

Alega la parte recurrente que, teniendo en cuenta todo lo expuesto anteriormente, y debido al hecho que concurren circunstancias excepcionales derivadas de la crisis económica generada por la pandemia y por la guerra de Ucrania, y la decisión extraordinaria que Glovo tuvo que adoptar para acogerse a un ERE, la sanción debería fijarse en ******CANTIDAD.7***.

Subsidiariamente, alega la parte recurrente que en aplicación del principio de proporcionalidad y de los criterios establecidos por las Directrices 04/2022, la sanción debería fijarse en el importe mínimo de ******CANTIDAD.5*** que resulta de la horquilla calculada según los criterios de los párrafos 61 y 67 de las Directrices 04/2022.

Al respecto, esta Agencia desea señalar que por los motivos detalladamente expuestos en los apartados anteriores, se desestima la presente alegación.

QUINTO.- ABUSO DE DERECHO POR PARTE DE LA AEPD Y EXISTENCIA DE RESPONSABILIDAD PATRIMONIAL

5.1. Existencia de abuso de derecho

Alega la parte recurrente que la AEPD abrió un nuevo procedimiento sancionador (el actual PS/00209/2022) tras haberse declarado la caducidad del anterior procedimiento (PS/00020/2021), y ello en base a unos hechos y fundamentos de derecho idénticos, lo cual ha creado, a su juicio, desde el primer momento una situación de inseguridad jurídica para Glovo evidente.

La parte recurrente insiste en que, tras declararse la caducidad de un procedimiento administrativo sancionador, no es de recibo que se abra otro procedimiento con base a los mismos hechos, puesto que no se puede sancionar, ni ser "juzgados" dos veces por lo mismo. En este sentido, añade que no puede ser tolerable que una Administración se aproveche de los efectos de su inactividad para poder argumentar que si "vuelve a sancionar", no se puede considerar que la primera vez se sancionó porque esa sanción "era nula de pleno derecho".

Por ello, alega la parte recurrente que un nuevo procedimiento en base a unos hechos y fundamentos de derecho idénticos no puede calificarse de otro modo que un acto claro de abuso de derecho por parte de esta Agencia dado que la caducidad, de ser un instrumento de garantía y tranquilidad del ciudadano, pasaría así a convertirse en un mero instrumento de la supuesta negligencia de los funcionarios; un instrumento que recae a fin de cuentas, sobre las espaldas de Glovo como administrado, que no sólo se vería sometido a la tortura (y, por cierto, también a los gastos) de un nuevo expediente y a la incertidumbre que entraña.

Al respecto, esta Agencia desea reiterar lo ya expuesto en la citada Resolución Sancionadora objeto del presente recurso.

En el presente caso, esta Agencia únicamente declaró la caducidad de las actuaciones en una única oportunidad (procedimiento número PS/00020/2021) por haber transcurrido el plazo de 9 meses previsto para su resolución en virtud del artículo 64.2 de la LOPDGDD e inició un nuevo procedimiento sancionador por infracciones que no estaban prescritas, tal y como lo prevé el artículo 95.3 de la LPACAP:

"*La caducidad no producirá por sí sola la prescripción de las acciones del particular o de la Administración, pero los procedimientos caducados no interrumpirán el plazo de prescripción.*

En los casos en los que sea posible la iniciación de un nuevo procedimiento por no haberse producido la prescripción, podrán incorporarse a éste los actos y trámites cuyo contenido se hubiera mantenido igual de no haberse producido la caducidad. En todo caso, en el nuevo procedimiento deberán cumplimentarse los trámites de alegaciones, proposición de prueba y audiencia al interesado."

No se trata, por tanto, en el presente caso de un supuesto en el que se reinicien varias veces un procedimiento tras sucesivas declaraciones de caducidad ni en el que pueda apreciarse la existencia de un abuso de derecho por parte de la Administración al tra-

tarse de una posibilidad precisamente prevista en la misma legislación que regula el procedimiento administrativo.

De hecho, es jurisprudencia consolidada del Tribunal Supremo la establecida en la STS 4084/2003, que dispuso: *"La declaración de caducidad y archivo de actuaciones establecidas para procedimientos en que la Administración ejercite potestades sancionadoras, artículo 44.2 de la Ley 30/1992, no extinguen la acción de la Administración para ejercitar las potestades aludidas en ese precepto, siéndoles plenamente aplicable el artículo 92.3 de la misma Ley*".

En este sentido, el artículo 44.2 de la Ley 30/1992, tras establecer que el vencimiento del plazo producía la caducidad del procedimiento de oficio, añadía: "*En estos casos, la resolución que declare la caducidad ordenará el archivo de las actuaciones, con los efectos previstos en el artículo 92".*

En igual sentido pueden citarse, previamente, entre otras, las sentencias STS 9569/2001, de 5 de diciembre y 2716/2002, de 17 de abril.

Alega la parte recurrente que una vez se declara la caducidad de un procedimiento no es de recibo que se proceda a la apertura de un nuevo procedimiento por el principio básico de *ne bis in idem*, es decir, porque no se puede sancionar, ni ser "juzgados" dos veces por un mismo hecho. En este sentido, entiende que no puede ser tolerable que una Administración se aproveche de los efectos de su inactividad para poder argumentar que si "vuelve a sancionar", no se puede considerar que la primera vez se sancionó porque esa sanción "era nula de pleno derecho".

Al respecto, esta Agencia desea señalar que la parte recurrente está haciendo referencia a un supuesto completamente distinto del planteado en el presente caso, toda vez que refiere a un supuesto en el que se había dictado sanción una vez transcurrido el plazo para ello, por lo que la sanción era nula de pleno derecho y, una vez recurrida, se declara su nulidad y se abre nuevo procedimiento sancionador por no estar prescrita la infracción.

En el presente caso, esta Agencia aún no había dictado resolución cuando declaró la caducidad de las actuaciones número PS/00020/2021 y tampoco dictó resolución sancionadora con posterioridad. Por tanto, no había resolución nula de pleno derecho alguna. Simplemente se limitó a declarar la caducidad de las actuaciones, a comprobar que las infracciones en cuestión no habían prescrito y a abrir un nuevo procedimiento sancionador, tal y como se prevé en el artículo 95.3 de la LPACAP.

Además, en el presente caso no se ha producido una demora en el procedimiento que hubiera causado que se reiniciasen los plazos de prescripción por haber estado paralizado durante más de seis meses por causas no imputables al presunto infractor (artículo 75 de la LOPDGDD). Ni tampoco esta Agencia ha esgrimido en ningún momento que se hubiera interrumpido el plazo de prescripción durante la duración del procedimiento sancionador número PS/00020/2021 ya caducado para poder iniciar el procedimiento sancionador objeto del presente recurso.

Simplemente se ha limitado a aplicar el ya citado artículo 95.3 de la LPACAP, que contempla la posibilidad de iniciar un nuevo procedimiento por no haberse producido citada prescripción de la infracción, como en el presente caso.

Y esta Agencia entiende que no puede hablarse de inseguridad jurídica ni de un claro abuso de derecho por parte de esta Agencia cuando es la misma ley que regula el procedimiento administrativo la que contempla la opción de iniciar un nuevo procedimiento sancionador si la infracción en cuestión no está prescrita, en caso de haberse caducado las actuaciones anteriores por no haber sido resuelto en el plazo previsto para ello.

Finalmente, esta Agencia desea señalar que no es objeto del presente procedimiento si la parte recurrente ha sufrido de “tortura” e “incertidumbre” ante su accionar, el cual en el presente caso siempre ha estado en cumplimiento con la normativa aplicable y hasta la doctrina consolidada del Tribunal Supremo.

Por todo lo expuesto, se desestima la presente alegación.

5.2. Existencia de responsabilidad patrimonial de la Administración

La parte recurrente recuerda a esta Agencia que, con independencia de haber tenido que involucrar a otras autoridades de control interesadas, es evidente que su inactividad provocó la caducidad del anterior procedimiento PS nº PS/00020/2021 y, en el presente procedimiento, ha conllevado que haya tenido que reiterar las alegaciones que ya presentó en su momento, con los correspondientes costes directos por honorarios de abogados, peritos y tiempo dedicado a la defensa.

Entiende que estos costes generados a Glovo constituyen un daño efectivo, evaluable económicamente e individualizado imputable a la AEPD, los cuales traen causa de un funcionamiento anormal de la Agencia debido a su clara inactividad.

Y reitera que se reserva las acciones necesarias para reclamar la responsabilidad patrimonial de la Administración por los daños y perjuicios causados por su inactividad.

Al respecto, esta Agencia desea reiterar lo ya expuesto en la citada Resolución Sancionadora objeto del presente recurso.

Esta Agencia desea resaltar que no es objeto del presente procedimiento la posibilidad o no de apreciar la responsabilidad patrimonial de la Administración, lo cual sería objeto de otro procedimiento, y esta Agencia pone de manifiesto que la parte recurrente es libre de realizar las acciones que considere necesarias a tal fin.

Si bien es cierto que parece difícil considerar que pueda caber responsabilidad patrimonial por el hecho de que la Administración actúe conforme a un supuesto expresamente prevista en la legislación procedimental, como es el ya mencionado artículo 95.3 de la LPACAP, que prevé la posibilidad expresa de iniciar un nuevo procedimiento por caducidad del anterior, si la infracción en cuestión no está prescrita (como en el presente caso).

Por todo lo expuesto, se desestima la presente alegación.

III
Conclusión

En consecuencia, en el presente recurso de reposición, la parte recurrente no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada.

IV
Resolución extemporánea

Debido a razones de funcionamiento del órgano administrativo, por ende no atribuibles a la parte recurrente, hasta el día de la fecha no se ha emitido el preceptivo pronunciamiento de esta Agencia respecto al presente recurso.

De acuerdo con lo establecido en el art. 24 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP) el sentido del silencio administrativo en los procedimientos de impugnación de actos y disposiciones es desestimatorio.

Con todo, y a pesar del tiempo transcurrido, la Administración está obligada a dictar resolución expresa y a notificarla en todos los procedimientos cualquiera que sea su forma de iniciación, según dispone el art. 21.1 de la citada LPACAP.

Por tanto, procede emitir la resolución que finalice el procedimiento del recurso de reposición interpuesto.

Vistos los preceptos citados y demás de general aplicación,
la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por GLOVOAPP23, S.A. contra la resolución de esta Agencia Española de Protección de Datos dictada con fecha 7 de marzo de 2023, en el expediente RR/00261/2023.

SEGUNDO: NOTIFICAR la presente resolución a GLOVOAPP23, S.A.

TERCERO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva una vez sea ejecutiva la presente resolución, de conformidad con lo dispuesto en el artículo 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida nº ES00 0000 0000 0000 0000 0000, abierta a nombre de la Agencia Española de Protección de Datos en el Banco CAIXABANK, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago

voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), los interesados podrán interponer recurso contencioso-administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada LPACAP. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

180-111122

Mar España Martí
Directora de la Agencia Española de Protección de Datos