- **Procedimiento Nº: PS/00225/2020**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: ***A.A.A.*** (en adelante, el reclamante) con fecha 15 de junio de 2019 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra GLOVOAPP23, S.L. con NIF B66362906 (en adelante, el reclamado). Los motivos en que basa la reclamación son que en febrero de 2018 solicitó la eliminación de su cuenta de la aplicación, a lo que le respondieron al correo electrónico con la confirmación de la recepción de su solicitud. No obstante, el 27 de mayo de 2019 recibió un correo electrónico de un pedido realizado con su cuenta, el cual no había sido realizado por el reclamante. Se puso en contacto con la empresa a través del correo electrónico y le contestaron "en un idioma extraño, con caracteres raros" solicitándole los datos de su tarjeta de crédito, que no les facilita. También contactó a través de Twitter e inicialmente le dijeron que la cuenta de su correo no existía, que el pedido en cuestión había sido cancelado y, posteriormente, ante su solicitud de acceso a la cuenta para borrar los datos bancarios, volvieron a pedirle la identificación con su DNI y tarjeta de crédito. Al enviarle los datos, le respondieron que necesitaban más datos de su tarjeta de crédito, a lo que él se opuso. Solicita que se eliminen sus datos "definitivamente de su Base de Datos, lo que ya han incumplido una vez".

Junto a la reclamación aporta, entre otra, la siguiente documentación:

- Intercambio de correos electrónicos con fecha 1 de febrero de 2018 en el que el reclamado, desde la dirección ***support@glovohelp.***EMPRESA.1.com***, le pide al reclamante a su dirección de correo electrónico ***EMAIL.1*** que responda a ese email para confirmar la baja y le indica que "Recuerda que una vez tramitada, todos tus datos serán borrados y no podrás volver a acceder al detalle de los glovos que hayas realizado". El reclamante responde con la confirmación de la baja y se le contesta que "Tu mensaje nº (***ID.4) se está gestionando para encontrar la mejor solución posible".
- Correo electrónico de fecha 27 de mayo de 2019, recibido en la cuenta de correo electrónico desde la que el reclamante solicitó la eliminación de su cuenta, de un "Pedido confirmado" escrito en letras de alfabeto cirílico, con número de identificación "ID: KI17LG1HM".
- Intercambio de correos electrónicos de fecha 27 de mayo de 2019 entre el reclamante y liveops.comms@glovoapp.com en el que denuncia que se ha hecho este pedido por otra persona, pero que los cuatro últimos dígitos de su tarjeta de crédito, que aparecen en el correo del pedido, coinciden con los de su tarjeta de crédito y que intentó conectarse a la aplicación pero le pidió confirmación al teléfono, que no coincide con su número. El reclamado "para garantizar un pago seguro" le solicita al reclamante que le envíe una copia de su DNI o pasaporte y de la tarjeta de crédito, en la que se vean únicamente el nombre del titular y los 6 primeros dígitos y 4 últimos dígitos. El reclamante responde que no quiere realizar ningún pago, que el último pedido no lo

realizó él y que le suplantaron la identidad, que no puede acceder a la cuenta y que no les va a enviar sus datos bancarios porque ve una falta de seguridad importante en la aplicación y solicita que se elimine esa cuenta.

- Correos electrónicos de fecha 6 de junio de 2019 enviados por liveops.comms@glovoapp.com al reclamante en los que se indica que la cuenta ha sido bloqueada por actividades sospechosas y le solicitan copia de su DNI o pasaporte y de la tarjeta en la que se vean únicamente el nombre del titular y los 6 primeros dígitos y 4 últimos dígitos con el objeto de comprobar la identidad para revisar el estado de la cuenta. Y correo electrónico de fecha 7 de junio de 2019 enviado por liveops.comms@glovoapp.com al reclamante en el que se le solicita que vuelva a enviar la copia de su tarjeta debido a que no se pueden visualizar los 6 primeros dígitos.
- Intercambio de mensajes en Twitter desde el 27 de mayo hasta el 8 de junio de 2019 en el que el reclamante expone que se ha realizado un pedido que él no ha solicitado, que está preocupado porque los últimos dígitos de la tarjeta de crédito coinciden con la suya, que quiso acceder a su cuenta y no pudo y que el teléfono para recuperar la contraseña no es el suyo. El reclamado en un principio le contesta que el correo electrónico facilitado no corresponde a ninguna cuenta y le solicitan un número de pedido que hubiera realizado en el pasado. El reclamante les facilita el número de pedido #GJPYLGSVC de fecha 6/1/2018 y el reclamado le contesta que le consta que el pedido no solicitado ha sido cancelado sin costes y que recibirá el importe cobrado incorrectamente. El reclamante insiste en que desea eliminar sus datos de la aplicación, para lo cual quiere acceder a la misma. Para ello, el reclamado le pide que realice “una verificación que le hemos enviado a su correo”. El reclamante reproduce el correo en el que le solicitan copia del DNI y copia de la tarjeta de crédito asociada a la cuenta en la que se vea su nombre y los 6 primeros dígitos y 4 últimos dígitos. El reclamante indica que envió la foto, pero el reclamado insiste en que en las imágenes adjuntadas no se pueden visualizar los primeros seis dígitos de la tarjeta y que necesitan esa información “para poder habilitar su perfil”. El reclamante se niega a facilitarle estos datos por desconfianza en la seguridad de la aplicación, toda vez que en febrero había pedido eliminar la cuenta y le habían contestado que lo harían, pero meses más tarde recibe un mensaje de que se hizo un pedido desde la cuenta que había solicitado eliminar. Expone que solo quería acceder a la aplicación para eliminar su número de tarjeta de crédito y que desea eliminar esa cuenta, junto con todos sus datos personales. Finalmente, el reclamado insiste en que necesita verificar su identidad “para proceder a la devolución del importe pagado y luego podremos cancelar la cuenta”. El reclamante contesta que primero le habían dicho que no existía una cuenta con su correo, luego que se ha bloqueado un pedido con su cuenta (la que le habían dicho que no existía), más tarde le dijeron que el dinero había sido devuelto y ahora le pedían más datos para devolverle el importe que ya estaba devuelto, que estaba claro que algo fallaba o que se contradecía el reclamado y que iba a presentar denuncia ante esta Agencia.

SEGUNDO: Tras la recepción de la reclamación, la Subdirección General de Inspección de Datos el 12/08/2019 dio traslado al reclamado de la reclamación presentada para su análisis y comunicación al reclamante de la decisión adoptada al

respecto. Igualmente, se le requería para que en el plazo de un mes remitiera a la Agencia determinada información:

- La decisión adoptada a propósito de esta reclamación.
- En el supuesto de ejercicio de los derechos regulados en los artículos 15 a 22 del RGPD, acreditación de la respuesta facilitada al reclamante.
- Informe sobre las causas que han motivado la incidencia que ha originado la reclamación.
- Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares, fechas de implantación y controles efectuados para comprobar su eficacia.
- Cualquier otra que considere relevante.

El 10/09/2019 tuvo entrada en esta Agencia la respuesta del reclamado con número de registro de entrada 042819/2019, en la que se aporta, entre otra, la siguiente información:

- Respecto a la decisión adoptada a propósito de esta reclamación: en primer lugar, el reclamado manifiesta que “el reclamante al haber consentido los Términos de Uso de la plataforma y haber consentido los términos de nuestra Política de Privacidad, acepta que, pertenece al propio usuario la obligación de demostrar que ejerció su derecho de tratamiento de sus datos personales en las formas establecidas en nuestra Política de Privacidad”. En segundo lugar, afirma que el reclamado, “en su calidad de Responsable del tratamiento, adoptó en su momento las medidas necesarias para proceder a la supresión de sus datos, no obstante, el artículo 17.3. e) del RGPD permite fundamentar la posibilidad de conservar los datos personales a pesar de que el usuario haya retirado su consentimiento para tratarlos, siempre y cuando dicha conservación se base en la necesidad de defender los intereses legales y administrativos de la empresa responsable del tratamiento”. Y que “el derecho de supresión no es un derecho automático, sino que deben cumplirse uno de los requisitos anteriormente detallados” en el art. 17.3 y que “el art. 17. 3.e) permite la conservación de los datos, entre otros casos, siempre y cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones”, como la del presente caso. En tercer lugar, indica que el reclamado actuó con la debida diligencia puesto que el reclamante recibió una respuesta a su correo electrónico mediante la cual se confirmaba la recepción de su solicitud, lo cual demuestra que se trata con atención la solicitud del reclamante y le mantiene informado sobre el estado de su solicitud. En cuarto lugar, afirma que el reclamado “ha adoptado las medidas de seguridad necesarias y adecuadas al nivel de riesgo existente para evitar las brechas, fugas y malos tratos de datos personales en su sistema de tratamiento” y que cuando un usuario de su aplicación móvil es víctima de un hackeo de su cuenta de correo electrónico, “no puede considerarse que dicho acceso no autorizado se deba a las presuntas carencias del sistema de seguridad de una aplicación” como la del reclamado, lo cual “ha sido reconocido y aceptado por el propio usuario, a la hora de descargarse la aplicación móvil” y al haber aceptado sus Términos y Condiciones y su Política de Privacidad. Por último, el reclamado indica que, además de cancelar el pedido supuestamente fraudulento y no facturárselo al reclamante, para reactivar su usuario en la aplicación se exige pasar ciertas medidas de seguridad, tales como facilitar datos personales y bancarios, los cuales el reclamante ha decidido no facilitar.

- Respecto al ejercicio de los derechos regulados en los artículos 15 a 22 del RGPD: el reclamado afirma que al solicitar al reclamante datos personales como su DNI o datos bancarios para poder acceder nuevamente a su cuenta, se puede comprobar que se ha cumplido correctamente con el RGPD, "congelando toda su información personal en nuestras bases de datos, una vez fue solicitada por el reclamante. Dicha congelación no significa supresión total, ya que de acuerdo con el art 17.3.e) esto podría producir una situación de desigualdad" entre reclamado y el reclamante.
- Respecto a las causas de la incidencia: el reclamado apunta como posible causa externa un acceso no autorizado al correo electrónico del usuario, víctima de un hackeo.
- Respecto a las medidas adoptadas para evitar incidencias similares: el reclamado enumera la congelación y pseudonimización de los datos del reclamante, de acuerdo con el citado art. 17.3.e); la cancelación del pedido supuestamente fraudulento, pese a que éste pudo deberse a un posible hackeo no atribuible al reclamado; y que se procedió a señalar y bloquear el perfil completo del usuario, con el fin de evitar posibles fraudes que pudieran afectarle.

El 26/09/2019, de conformidad con el artículo 65 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante contra el reclamado.

TERCERO: A la vista de los hechos anteriormente reseñados, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD) y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo, LOPDGDD).

Como resultado de las actuaciones de investigación practicadas, se constata que el responsable del tratamiento es el reclamado.

Asimismo, los días 12 de febrero y 4 de marzo de 2020 se realizó una inspección presencial en la sede del reclamado, en la que se obtuvo, entre otra, la siguiente información, según se desprende del informe de actuaciones previas de fecha 13/08/2020:

- El reclamado manifestó que, a finales del año 2018, se incluyó una medida de seguridad en su aplicación que consistía en que, siempre que un usuario se autentique desde un nuevo dispositivo, se le envía un código de verificación al teléfono móvil que hubo introducido durante el proceso de alta. Este proceso ya se utilizaba durante el proceso de alta para verificar que el número de teléfono introducido estaba en posesión del usuario.
- El reclamado manifestó que, tras la realización de cada pedido, se verifica automáticamente si la operación corresponde con algún patrón de intento de fraude y, en el caso de ser así, aparece una alerta para que un empleado del investigado bloquee la cuenta manualmente y alguien del departamento de fraude le solicite más información al usuario vía correo electrónico con el

objeto de levantar el bloqueo de la cuenta. Mientras dura el bloqueo de la cuenta, si el usuario intenta acceder a su cuenta, se le muestra un mensaje de aviso indicando que contacte con atención al cliente; este mensaje se observa en el ejemplo de captura de pantalla aportada durante la inspección.

- El reclamado manifestó que los datos de las cuentas cuyos usuarios han solicitado la supresión o que hayan sido bloqueadas por sospecha de fraude se conservan durante los plazos establecidos por motivos contables, operativos, fiscales y de prescripción de delitos y de las infracciones de la normativa de prevención de blanqueo de capitales.
- El reclamado manifestó que, de las tarjetas de crédito, sólo se almacenan en sus sistemas de información los 6 primeros y los cuatro últimos dígitos; el resto de datos de la tarjeta de crédito sólo los ha podido conocer el propio usuario y su proveedor del servicio de pasarela de pagos.
- El reclamado manifestó que el reclamante solicitó la baja de su cuenta de usuario pero no llegó a confirmar esa baja; y que la cuenta se bloqueó cuando el reclamado tuvo conocimiento de que esta cuenta pudo ser objeto de fraude, y, posteriormente, la cuenta de usuario fue borrada.
- La cuenta de usuario con la que supuestamente se hizo el pedido el 27 de mayo de 2019 tiene como fecha de creación en los sistemas de información del reclamado el 1 de junio de 2018, y como fecha de borrado el 10 de septiembre de 2019. Esto se desprende las capturas de pantalla realizadas durante la inspección en la base de datos y en la plataforma de administración del investigado sobre el pedido KI17LG1HM y los datos del cliente ***ID.4, asociados a ese pedido.
- En el momento de realizar la inspección, los datos del cliente ***ID.4, asociados al pedido realizado el 27 de mayo de 2019, estaban marcados como “FRAUD DELETED” y se habían seudonimizado, sin aparecer el nombre ni los apellidos del cliente en la plataforma de administración, lo cual se desprende de la captura de pantalla de los datos del cliente ***ID.4 en la plataforma de administración del reclamado.
- En el escrito presentado en nombre del reclamado, con fecha de entrada en la AEPD el 17 de julio de 2020 y número de registro de entrada 025445/2020, se declara lo siguiente: Que tras la supresión de los datos, para demostrar la trazabilidad del protocolo llevado a cabo, se creó ad hoc un perfil nuevo sin datos personales; por este motivo, la fecha de creación aportada coincide con la fecha de supresión de la cuenta.

CUARTO: Con fecha 1 de septiembre de 2020**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción del Artículo 6.1 del RGPD, tipificada en el Artículo 83.5.a) del RGPD.

QUINTO: Notificado el citado acuerdo de inicio, el reclamado presentó escrito de alegaciones de fecha 30 de septiembre de 2020 en el que, en síntesis, manifestaba que “los hechos ocurridos en relación con la cuenta del usuario reclamante coinciden plenamente con el patrón de actuación habitual de los ciberdelincuentes que utilizan los datos comercializados en el mercado negro de países de la Europa del Este como Ucrania para suplantar la identidad de sus víctimas y realizar compras fraudulentas.

En este caso concreto, veremos que el ciberataque se realiza desde Ucrania y que aprovecha la actuación negligente del reclamante, al utilizar reiteradamente la misma clave en distintos servicios que fueron afectados por una brecha de seguridad que dejó expuestas sus credenciales.

Tras las distintas hipótesis analizadas en la investigación, mi representada ha llegado a la conclusión de que estas credenciales fueron utilizadas por el reclamante y posteriormente por el atacante en sucesivas cuentas de Glovo".

"El sitio web haveibeenpwned.com ofrece un servicio gratuito que permite a cualquier usuario comprobar si su dirección de correo electrónico figura en estas listas, y por lo tanto, si sus claves han quedado comprometidas y debe cambiarlas de inmediato. Si introducimos la dirección ***EMAIL.1** en esta base de datos, se comprueba que las credenciales del reclamante han quedado expuestas en cinco brechas de seguridad y dos intentos o indicios de ataque".

"Ello significa que la dirección de correo electrónico y las claves de acceso del reclamante han quedado expuestas en cinco brechas de seguridad o divulgaciones de datos de distintos servidores:
● Tres brechas de seguridad anteriores a la apertura de la cuenta en Glovo.
● Una lista de datos expuestos descubierta con anterioridad a la apertura de la cuenta en Glovo.
● Una lista de datos enriquecidos descubierta con posterioridad a la apertura de la cuenta en Glovo, pero con datos que tenían una antigüedad superior. Adjuntamos como DOCUMENTO UNO el informe relativo a estas brechas de seguridad".

También alega el reclamado que "La investigación también demostró que el reclamante tenía abierta otra cuenta en Glovo con la dirección ***EMAIL.2**, domicilio de entrega y tarjeta de crédito (dígitos iniciales y finales coincidentes). Utilizando el mismo recurso se comprueba que esta dirección quedó expuesta en nueve brechas de seguridad".

"Los ciberataques basados en listas de credenciales adquiridas en el mercado negro explotan la negligencia de los usuarios que utilizan las mismas claves de acceso en los distintos servicios online que contratan.

Ello justificaría el hecho de que las credenciales del reclamante apareciesen en listas enriquecidas. Las listas enriquecidas incluyen los datos que han sido verificados y que han sido completados con las aportaciones de otros ciberdelincuentes que los han explotado con éxito.

El resultado final es que los datos del reclamante inicialmente expuestos en estas listas se limitaban a la dirección de correo electrónico y a la clave de acceso, y, en las últimas versiones de 2019 los datos del reclamante habían sido enriquecidos con muchos más datos, que incluyen:

1. Ubicación geográfica
2. Datos de empleo
3. Números de teléfono

4. Perfiles en redes sociales
5. Tarjetas de crédito”

“Ello lo convierte en un exponente de escasa diligencia en la gestión y custodia de sus credenciales, ya que su historial de claves expuestas en brechas de seguridad se inicia en 2008 y llega hasta 2019, y el éxito de la suplantación de identidad confirma que durante todo este tiempo el reclamante no ha cambiado las claves de acceso reiteradamente comprometidas.

En los Términos y Condiciones que regulan el servicio, disponibles en https://glovoapp.com/es/legal/terms, Glovo advierte a los usuarios de su responsabilidad con respecto a la elección de sus contraseñas y al usar la app de Glovo el usuario acepta expresamente estas obligaciones:

“Cláusula 17. - Los Usuarios son completamente responsables del acceso y correcto uso de su perfil y demás contenidos de la Plataforma con sujeción a la legalidad vigente, sea nacional o internacional del País desde el que hace uso de la Plataforma, así como a los principios de buena fe, a la moral, buenas costumbres y orden público. Y específicamente, adquiere el compromiso de observar diligentemente las presentes Condiciones Generales de Uso.

Los Usuarios son responsables de consignar correctamente nombres de usuario y contraseñas individuales, no transferibles y lo suficientemente complejas, así como no usar el mismo nombre de usuario y contraseña que en otras plataformas, todo ello con la finalidad de proteger su cuenta del uso fraudulento por parte de terceros ajenos a la plataforma. (...)”

El reclamado en sus alegaciones plantea cuatro líneas posibles de investigación:

“El cambio de la aplicación de CRM destinada a recopilación de todas las acciones y transacciones de los clientes impide a mi representada tener los logs con los detalles de las operaciones realizadas en 2018, por lo que la investigación se ha centrado en verificar o refutar las cuatro hipótesis de trabajo que desarrollaremos en los siguientes puntos, demostrando que la actuación de Glovo ha sido diligente en los cuatro escenarios.

1. Primera hipótesis. - El ciberatacante utilizó las credenciales del reclamante, desbloqueó y restauró la cuenta anterior.

2. Segunda hipótesis. - El reclamante nunca verificó su número de teléfono móvil y el doble factor de autenticación quedó sin activar. Es posible que una cuenta que se quede inactiva durante unos meses (dormant account), pase a un modo de semibloqueo y no reaccione a la orden de supresión.

3. Tercera hipótesis. - El ciberatacante creó una nueva cuenta utilizando la dirección de correo electrónico y los datos de la tarjeta de crédito del reclamante, obtenidos en el mercado negro.

4. Cuarta hipótesis. - El reclamante abrió una nueva cuenta después de la supresión de la anterior.”

Respecto a la primera hipótesis (que el ciberatacante utilizó las credenciales del reclamante y restauró la cuenta anterior),el reclamado enumera en sus alegaciones una serie de requisitos que debieron cumplirse y concluye que el reclamado realizó la supresión y el bloqueo de los datos del reclamante de forma correcta y que comunicó la supresión al reclamante, para lo cual aporta como DOCUMENTO 2 la captura de la pantalla extraída de la copia de seguridad, en la que aparece esta confirmación.

En este Documento 2, adjunta una tabla en la que se puede observar, entre otra, la siguiente información:

id	subject	submitter	comment	Message created at
***ID.4	Eliminación de cuenta	{'id': 116472211014, 'url': 'https://glovoservice.***EMPRESA.1*.com/api/v2/users/116472211014.json', 'name': '***A.A.A.***', 'email': ***EMAIL.1', 'created_at': '2018-01-	Hola, he estado buscando tanto en la aplicación cómo en la página web, y no he encontrado en ningún sitio forma de eliminar la cuenta. Entiendo que esto debería ser posible de una forma sencilla (aunque esté escondido), y si no puede ser desde la App que fuese desde la página web. ¿Pueden decirme cómo debo proceder al respecto?	2018-02-01T19:39:34.000Z
***ID.4	Eliminación de cuenta	{'id': 116472211014, 'url': 'https://glovoservice.***EMPRESA.1*.com/api/v2/users/116472211014.json', 'name': '***A.A.A.***', 'email': ****EMAIL.1***', 'created_at': '2018-01-	¡Hola ***A.A.A.***! Las despedidas siempre son duras, ¡no queremos que te vayas! :(, aunque nos gustaría saber el motivo por el cual has decidido irte, ¡nos importa tu opinión! Si ya te lo has pensado bien y quieres eliminar tu cuenta, responde a este email confirmando la baja y gestionaremos tu petición a la mayor brevedad posible. Recuerda que una vez tramitada, todos tus datos serán borrados y no podrás volver a acceder al detalle de los	2018-02-01T19:40:28.000Z
***ID.4	Eliminación de cuenta	{'id': 116472211014, 'url': 'https://glovoservice.***EMPRESA.1*.com/api/v2/users/116472211014.json', 'name': '***A.A.A.***', 'email': ****EMAIL.1'***, 'created_at':	Confirmo la eliminación, gracias Un saludo El 1 feb 2018, a las 20:40, Glovo <support@glovohelp.***EMPRESA.1.com> escribió:	2018-02-01T19:44:18.000Z
***ID.4	Eliminación de cuenta	{'id': 116472211014, 'url': 'https://glovoservice.***EMPRESA.1*.com/api/v2/users/116472211014.json',		2018-02-01T19:49:22.000Z

		'name': '***A.A.A.***', 'email': ******EMAIL.1***', 'created_at':	solved en ***ID.4	
1511051	Eliminación de cuenta	360237355414, 'url': 'https://glovoservice.******EMPRESA.1***.com/api/v2/users/360237355414.json', 'name': '***A.A.A.***', 'email':	Quiero eliminar mi cuenta de Glovo ---------- Enviado desde: https://glovoapp.com/es/contact	2018-02-01T19:45:30.000Z
1511051	Eliminación de cuenta	{'id': 360237355414, 'url': 'https://glovoservice.******EMPRESA.1***.com/api/v2/users/360237355414.json', 'name': '***A.A.A.***', 'email': '******EMAIL.3***	¡Hola ***A.A.A.***! Las despedidas siempre son duras, ¡no queremos que te vayas! :(, aunque nos gustaría saber el motivo por el cual has decidido irte, ¡nos importa tu opinión! Si ya te lo has pensado bien y quieres eliminar tu cuenta, responde a este email confirmando la baja y gestionaremos tu petición a la mayor brevedad posible.	2018-02-01T19:47:18.000Z
1511051	Eliminación de cuenta	360237355414, 'url': 'https://glovoservice.******EMPRESA.1***.com/api/v2/users/360237355414.json', 'name': '***A.A.A.***', 'email':	El 1 feb 2018, a las 20:47, Glovo <support@glovohelp.***EMPRESA.1.com> escribió:	2018-02-01T19:47:56.000Z
1511051	Eliminación de cuenta	{'id': 360237355414, 'url': 'https://glovoservice.******EMPRESA.1***.com/api/v2/users/360237355414.json', 'name': '**A.A.A.**', 'email': '*****EMAIL.3**	¡Hola ***A.A.A.***! Ya no hay vuelta atrás :(Te confirmamos que hemos eliminado tu cuenta de usuario de nuestra base de datos. Tal y como te comentamos, ya no podrás acceder a tu perfil ni al detalle de tus pedidos anteriores. La baja del envío de la newsletter a tu correo electrónico se hará efectiva en aproximadamente unas 48 horas hábiles	2018-02-01T19:48:43.000Z
***ID.5	Eliminación de cuenta	{'id': 116018503873, 'url': 'https://glovoservice.******EMPRESA.1***.com/api/v2/users/116018503873.json', 'name': ***'A.A.A.***, 'email': ***'***EMAIL.2***	Quiero borrar mi cuenta, vinculada a través de Facebook, Gracias un saludo ---------- Enviado desde: https://glovoapp.com/es/contact	2018-02-01T19:46:23.000Z
***ID.5	Eliminación de cuenta	{'id': 116018503873, 'url': 'https://glovoservice.******EMPRESA.**	¡Hola ***A.A.A.***! Las despedidas siempre son duras, ¡no queremos que te vayas! :(, aunque nos gustaría saber el motivo por el cual has decidido irte, ¡nos importa tu opinión! Si ya te lo has pensado bien y	2018-02-01T19:48:10.000Z

		1.com/ api/v2/users/116 018503873.json', 'name': **'A.A.A.'**, 'email': ***'***EMAIL.2***	quieres eliminar tu cuenta, responde a este email confirmando la baja y gestionaremos tu petición a la mayor brevedad posible. Recuerda que una vez tramitada, todos tus datos serán borrados y no podrás volver a acceder al detalle de los	
***ID.5	Eliminación de cuenta	{'id': 116018503873, 'url': 'https://glovoservice.***EMPRESA.1***.com/ api/v2/users/116 018503873.json', 'name': '***A.A.A.***', 'email': ***'***EMAIL.2***	Confirmo la eliminación de la cuenta, un saludo El 1 feb 2018, a las 20:48, Glovo <support@glovohelp.***EMPRESA.1.com> escribió:	2018-02-01T19:48:48.000Z
***ID.5	Eliminación de cuenta	{'id': 116018503873, 'url': 'https://glovoservice.***EMPRESA.1***.com/ api/v2/users/116 018503873.json', 'name': ***'A.A.A'***, 'email': ***'***EMAIL.2***	¡Hola ***A.A.A.***! Ya no hay vuelta atrás :(Te confirmamos que hemos eliminado tu cuenta de usuario de nuestra base de datos. Tal y como te comentamos, ya no podrás acceder a tu perfil ni al detalle de tus pedidos anteriores. La baja del envío de la newsletter a tu correo electrónico se hará efectiva en aproximadamente unas 48 horas hábiles. Si tienes cualquier otra consulta al respecto, no dudes en contactarnos respondiendo a este mismo email.	2018-02-01T19:52:54.000Z

Indica el reclamado que para haber realizado el pedido fraudulento, el ciberdelincuente debería haber conseguido permisos de administrador y realizado todos los pasos descritos y haber sorteado todos los obstáculos establecidos para impedirlo.

También señala que sería absolutamente desproporcionado organizar un ataque tan potente para realizar un pedido minúsculo.

Por todo ello el reclamado concluye que esta primera hipótesis debe ser rechazada.

También señala el reclamado la posibilidad de que la confusión generada por la duplicidad de cuentas del reclamante y el ejercicio del derecho de supresión limitado a una de ellas hiciese que la otra quedase operativa y fuese esa la que el atacante utilizó para suplantar la identidad del reclamante.

Respecto a la segunda hipótesis (el reclamante nunca verificó su número de teléfono móvil y el doble factor de autenticación quedó sin activar. Es posible que una cuenta que se quede inactiva durante unos meses (dormant account), pase a un modo de semibloqueo y no reaccione a la orden de supresión), el reclamado alega que “una cuenta no verificada y sin el doble factor activado coincide con un patrón de intento de fraude y por tanto se bloquea la cuenta. Este bloqueo sería distinto del bloqueo post supresión, ya que en los intentos de fraude los datos bloqueados siguen en la base de datos principal porque deben ser consultados por el equipo antifraude para prevenir nuevos intentos de fraude.

Sin embargo, esta hipótesis no encaja con el hecho de que mi representada verificó y confirmó en febrero de 2018 que la cuenta había sido correctamente suprimida".

"En cualquier caso, el bloqueo derivado de una sospecha de fraude, justifica que los datos se mantengan en la base de datos principal, ya que sirven para verificar nuevos intentos de fraude que provengan de la misma cuenta de correo electrónico, el mismo móvil o las mismas cifras finales de la tarjeta de crédito.

Mi representada entiende que el mantenimiento de los datos sospechosos de haber participado en un intento de fraude es una finalidad correcta y necesaria para proteger al propio cliente, que justificaría su conservación en la base de datos principal tras la solicitud de supresión del reclamante".

Respecto a la tercera hipótesis (el ciberatacante creó una nueva cuenta utilizando la dirección de correo electrónico y los datos de la tarjeta de crédito del reclamante, obtenidos en el mercado negro), el reclamado alega que "La AEPD constató, en el transcurso de la inspección en Glovo, y lo considera como un hecho probado, que el pedido fraudulento se realizó con una cuenta que había sido creada el 1 de junio de 2018. Ello se repite varias veces en el acuerdo de inicio de procedimiento sancionador y en las actas de la inspección.

Este dato es muy importante, porque demuestra que la cuenta con la que se realizó el pedido fraudulento no fue la misma que creó el reclamante. ES UNA CUENTA DISTINTA.

La primera cuenta tenía el ID ***ID.1 y la segunda el ID ***ID.3.

Además, la primera cuenta utilizó una tarjeta MASTERCARD y la segunda una tarjeta VISA.

Recordemos que los hechos probados se inician en febrero de 2018, cuando el reclamante solicita la eliminación de su cuenta y la supresión de sus datos.

Sin embargo, las comprobaciones realizadas por la AEPD demuestran que la cuenta utilizada para realizar el pedido fraudulento fue creada CUATRO MESES DESPUÉS de que el reclamante solicitase la cancelación de su cuenta y Glovo procediese a suprimir y bloquear los datos.

Entendemos que fue el ciberdelincuente el que abrió esa cuenta en junio de 2018 con los datos que había obtenido en las listas de direcciones de correo electrónico que se venden en internet y en el mercado negro.

Ello acreditaría que la supresión de la cuenta y el bloqueo de los datos se realizó correctamente, ya que, de lo contrario el ciberdelincuente no habría podido utilizar la misma dirección de correo electrónico".

El reclamado indica que, para que esta hipótesis fuese factible, deberían haberse cumplido los siguientes requisitos:

Paso	Requisito obligatorio	Obstáculos
Acceso a la cuenta	Apertura de nueva cuenta	No existen obstáculos para la creación de una nueva cuenta porque la dirección de correo electrónico del reclamante había sido suprimida y no se producía una duplicidad de cuenta.
Verificación mediante doble factor de autenticación	Envío de SMS al móvil y aceptación del usuario	El ciberdelincuente utilizó su propio móvil para instalar la aplicación y la nueva cuenta. Recibió el SMS en él y la cuenta quedó verificada. **Esta verificación está acreditada y se produjo el 27 de mayo de 2019 a las 11:14 pm CEST, de acuerdo con el log del sistema.** Adjuntamos como DOCUMENTO TRES el log de verificaciones. Por eso el reclamante no recibió un SMS de verificación y por eso el reclamante vio que el número de móvil de la cuenta no coincidía con el suyo.
Modificación del domicilio	Modificación de datos que estaban bloqueados y trazabilidad de la modificación	Al ser una cuenta nueva, el ciberdelincuente puso el domicilio que consideró oportuno para la entrega.
Pago del pedido	Acceso al medio de pago	El ciberdelincuente obtuvo los datos de la tarjeta asociada a la dirección de correo electrónico del reclamante en el mercado negro.

El reclamado también alega que es notorio y ampliamente conocido que, en el mercado negro de la Internet profunda, se pueden adquirir datos de tarjetas de crédito que han quedado expuestas y que se pueden adquirir listas de cuentas con tarjetas de crédito no anuladas tras una brecha de seguridad. Y que el reclamado defiende que el ciberatacante obtuvo los datos de la tarjeta de crédito asociada a la dirección de correo del reclamante en una de estas listas.

Para ello, resalta dos hechos:

1. El reclamante sufrió una brecha de seguridad en su cuenta de Dropbox, donde podía conservar los datos de su tarjeta de crédito.

2. Los datos del reclamante figuraban en la lista enriquecida que fue descubierta en 2019, pero que contenía datos de una antigüedad superior, que habían sido enriquecidos con aportaciones de otros ciberdelincuentes.

Señala el reclamado que Ucrania es también un país históricamente relacionado con el phishing, por lo que la facilidad para acceder a datos de tarjetas de crédito es muy superior a la de otros países. Y que, por todo ello, considera que la opción más probable es que el ciberdelincuente utilizase los datos de la tarjeta de crédito del reclamante para realizar el pedido fraudulento, dado que las otras opciones son mucho menos probables.

El reclamado destaca también que el cargo relativo al pedido fraudulento nunca llegó a realizarse, ya que fue Glovo la que detectó un patrón sospechoso y bloqueó el pago, por lo que en ningún momento se causaron perjuicios al reclamante.

Finalmente, el reclamado indica que, de acuerdo con las evidencias que constan en el procedimiento, obtenidas durante la inspección en las oficinas de Glovo, y aportadas por el reclamante y por el reclamado, la cronología de los hechos es la siguiente:

Año	Descubrimiento de las claves de acceso del reclamante en listas de claves
2012	Las claves de acceso de la cuenta del reclamante en Dropbox quedan expuestas
2016	Las claves de acceso de la cuenta del reclamante en LinkedIn quedan expuestas
2016	Las claves de acceso del reclamante aparecen en la lista Exploit.In
2019	Las claves de acceso del reclamante aparecen en la lista Collection 1#
2019	Las claves de acceso y otros datos del reclamante aparecen en una lista enriquecida

Año	Hechos
02/2018	El reclamante solicita la supresión de su cuenta y de sus datos
02/2018	Glovo suprime la cuenta y los datos y conserva una copia bloqueada en el datawarehouse
06/2018	El ciberdelincuente crea una cuenta en Glovo con los datos del reclamante
05/2019	El ciberdelincuente realiza un pedido fraudulento
05/2019	El reclamante recibe un mensaje de confirmación del pedido y lo comunica a Glovo

Y alega que “Esta cronología encaja perfectamente con los hechos probados y demuestra que mi representada actuó diligentemente y sin infringir la normativa de protección de datos.

La simple posibilidad de que los hechos se hayan producido de esta manera y no como la Agencia sostiene, pero no acredita, permite a mi representada acogerse al principio de presunción de inocencia administrativa y adopta como hipótesis más verosímil la relativa a la creación de una nueva cuenta por parte del atacante, que en ningún momento ha sido contradicha por la Agencia”.

Respecto a la cuarta hipótesis (el reclamante abrió una nueva cuenta después de la supresión de la anterior), el reclamado indica que esta hipótesis no sería descabellada, ya que, además de la cuenta de Glovo ******EMAIL.1***, el reclamante disponía de la cuenta ******EMAIL.2***, de la cual había olvidado su existencia, o al menos solo ejercitó el derecho de supresión en relación a una de ellas.

“Por ello, y a pesar de que los logs del sistema no conservan los datos de junio de 2018 para comprobar la dirección IP desde la que se produjo la apertura de esta nueva cuenta, es perfectamente factible que el reclamante abriese una nueva cuenta el 1 de junio de 2018 y después se olvidase de que la había abierto.

Esta hipótesis encajaría plenamente con la supresión inicial de los datos y la posterior suplantación de identidad por parte del ciberdelincuente, ya que los datos de la segunda cuenta abierta por el reclamante no habrían sido suprimidos.

Recordemos que los ID de las dos cuentas eran diferentes y las tarjetas de crédito también.

La cronología de los hechos relativa a esta hipótesis sería la siguiente:

Año	Hechos
02/2018	El reclamante solicita la supresión de su cuenta y de sus datos
02/2018	Glovo suprime la cuenta y los datos y conserva una copia bloqueada en el datawarehouse
06/2018	El reclamante crea una nueva cuenta
05/2019	El ciberdelincuente accede a la nueva cuenta con los datos del reclamante
05/2019	El ciberdelincuente realiza un pedido fraudulento
05/2019	El reclamante recibe un mensaje de confirmación del pedido y lo comunica a Glovo

Esta cronología también encaja con los hechos probados y demuestra que mi representada actuó diligentemente y sin infringir la normativa de protección de datos.

También en esta hipótesis, la simple posibilidad de que los hechos se hayan producido de esta manera y no como la Agencia sostiene, pero no acredita, permite a mi representada acogerse al principio de presunción de inocencia administrativa y adopta como hipótesis más verosímil la relativa a la creación de una nueva cuenta por parte del reclamante, que en ningún momento ha sido contradicha por la Agencia".

El reclamado también alega que ha realizado las siguientes acciones de mejora desde 2018:

"1. Cambio del software de CRM con el que se gestiona la relación con los clientes, pasado de la aplicación ******EMPRESA.1*** a ******EMPRESA.2***.

2. Mantenimiento y mejora de la plataforma que previene las acciones de fraude y bloquea los intentos que respondan a un patrón sospechoso.

3. Mantenimiento y mejora del doble factor de autenticación, eliminando el riesgo relativo a las cuentas inactivas cuyo teléfono móvil no fue verificado y el doble factor no fue activado.

4. Seudonimización de los datos bloqueados por sospecha de fraude.

5. Aplicación de las medidas de verificación de usuarios con dos cuentas a raíz del caso ******CASO.1***, que también llegó a la AEPD."

Señala también el reclamado que "en cada una de las hipótesis de trabajo barajadas Glovo actuó con sujeción a la ley y que en ningún caso mantuvo los datos del reclamante accesibles a personas diferentes de las autorizadas para acceder a los datos bloqueados en el datawarehouse.

Diferentes firmas de reconocido prestigio han emitido, con carácter previo al cierre de cada una de las rondas de financiación, informes de situación sobre el cumplimiento normativo de la compañía (Due Diligence). Mi representada ha cumplido puntualmente las recomendaciones contenidas en dichos informes con el fin de asegurar la protección de los derechos y libertades de los interesados.

En ninguno de estos informes se ha indicado que Glovo disponga de unas medidas de seguridad insuficientes en relación con el proceso de autenticación de los usuarios".

Finalmente, el reclamado señala que “considera no ajustada a Derecho la aplicación de los criterios agravantes que se han tenido en cuenta en el momento de graduar la sanción.

1. En relación con el carácter continuado de la infracción, mi representada ha acreditado que la cronología de los hechos sostenida por la AEPD no se corresponde con la realidad y que no se ha producido infracción alguna.

2. En relación con la cuantía de los usuarios, esta es errónea, ya que la cifra es muy inferior y a los efectos de este procedimiento deben tenerse en cuenta únicamente las cuentas activas. Si fuese cierto que mi representada trata los datos de más de 7 millones de clientes activos, sería un gran éxito haber tenido un único incidente de estas características, ya que por simple probabilidad estadística, los errores humanos o informáticos arrojan cifras de incidentes muy superiores”.

Y que “entiende que ha quedado debidamente demostrado que Glovo ha actuado en todo momento de buena fe, empleando su mayor compromiso, y sin nunca poner en peligro los derechos y libertades de los interesados. No existe, pues, una clara “intencionalidad” en incumplir con la normativa vigente ya que, mi representada realizó todas las acciones necesarias y debidas para el cumplimiento de la normativa y ha ajustado prudentemente su actuación a la ley”.

Solicita entonces:

- Que se tengan por interpuestas las alegaciones al acuerdo de apertura de procedimiento sancionador y se archive el Procedimiento PS/00225/2020.

- Que no se apliquen los criterios agravantes mencionados en dicho acuerdo.

- Que se reduzca en un 25% la sanción inicialmente propuesta por haber actuado la compañía en todo momento de buena fe, sin haber puesto en peligro los derechos y libertades de los interesados.

- Que se aplique una reducción de un 25% por pronto pago, aplicándose de forma acumulativa ambas reducciones.

SEXTO: Con fecha 12 de febrero de 2021, el instructor del procedimiento acordó la apertura de un período de práctica de pruebas, teniéndose por incorporados la reclamación interpuesta por el reclamante y su documentación, los documentos obtenidos y generados por los Servicios de Inspección ante el reclamado, el Informe de actuaciones previas de Inspección que forman parte del expediente E/10306/2019, así como las alegaciones al acuerdo de inicio PS/00225/2020 presentadas por el reclamado y la documentación que a ellas acompaña.

Con fecha 15 de febrero de 2021 la AEPD ha requerido al reclamado para que en el plazo de diez días hábiles presentara la siguiente información:

1) Capturas de pantalla con el procedimiento de búsqueda que permita identificar que la cuenta de usuario de Glovo con ID ***ID.1 estaba asociada a la dirección de correo

electrónico ***EMAIL.1***. Descripción detallada del procedimiento de búsqueda realizado en este punto.

2) Capturas de pantalla con el procedimiento de búsqueda que permita identificar la fecha de creación de la cuenta de usuario de Glovo con ID ***ID.1. Descripción detallada del procedimiento de búsqueda realizado en este punto.

3) Capturas de pantalla con el procedimiento de búsqueda que permita identificar la fecha de bloqueo de la cuenta de usuario de Glovo con ID ***ID.1. Descripción detallada del procedimiento de búsqueda realizado en este punto.

4) Capturas de pantalla con el procedimiento de búsqueda que permita identificar la fecha de supresión de la cuenta de usuario de Glovo con ID ***ID.1. Descripción detallada del procedimiento de búsqueda realizado en este punto.

Con fecha 10 de marzo de 2021, el reclamado presentó escrito de respuesta ante esta Agencia, en el que manifestaba que "con base a la información que consta en nuestros sistemas de información, la cuenta de usuario de Glovo asociada a la dirección de correo electrónico ***EMAIL.1** no corresponde al ID ***ID.1, sino al ID ***ID.4".

Y que "toda la información que se proporcione a esta Agencia mediante el presente escrito corresponde a la cuenta de usuario de Glovo asociada a la dirección de correo electrónico ***EMAIL.1** identificada en los sistemas de información de mi representada con el ID ***ID.4".

A continuación, el reclamado aporta la información requerida, pero respecto de la cuenta de Glovo ID ***ID.4.

Con fecha 18 de marzo de 2021 la AEPD ha requerido al reclamado para que en el plazo de diez días hábiles presentara la siguiente información:

1) Capturas de pantalla con el procedimiento de búsqueda que permita identificar el ID de la cuenta de usuario de Glovo de la consulta id***ID.4, asociada a la dirección de correo electrónico ***EMAIL.1***. Descripción detallada del procedimiento de búsqueda realizado en este punto.

2) Capturas de pantalla con el procedimiento de búsqueda que permita identificar la fecha de creación de la cuenta de usuario de Glovo de la consulta id***ID.4, asociada a la dirección de correo electrónico ***EMAIL.1***. Descripción detallada del procedimiento de búsqueda realizado en este punto.

3) Capturas de pantalla con el procedimiento de búsqueda que permita identificar la fecha de bloqueo de la cuenta de usuario de Glovo de la consulta id***ID.4, asociada a la dirección de correo electrónico ***EMAIL.1***. Descripción detallada del procedimiento de búsqueda realizado en este punto.

4) Capturas de pantalla con el procedimiento de búsqueda que permita identificar la fecha de supresión de la cuenta de usuario de Glovo de la consulta id***ID.4, asociada a la dirección de correo electrónico ***EMAIL.1***. Descripción detallada del procedimiento de búsqueda realizado en este punto.

Todo ello basado en que en su escrito de alegaciones de fecha 30/09/2020, número de registro de entrada O00007128e2000003988, GLOVOAPP23, SL alega en la página 5 que: “La investigación realizada por mi representada concluye que Glovo realizó la supresión y el bloqueo de los datos del reclamante de forma correcta y que comunicó la supresión al reclamante. Se aporta como DOCUMENTO 2 la captura de la pantalla extraída de la copia de seguridad, en la que aparece esta confirmación”. Y que en el Documento 2 que acompaña a esas alegaciones, en las primeras cuatro filas consta una consulta id***ID.4 y la cronología de la misma, en la que figura que dicha consulta id***ID.4 estaba asociada a la dirección de correo electrónico ******EMAIL.1***.

Con fecha 12 de abril de 2021, el reclamado presentó escrito de respuesta ante esta Agencia, en el que manifestaba que “la información adicional específica requerida por esta Agencia relativa específicamente a la consulta con ID***ID.4 asociada a la dirección de correo electrónico ******EMAIL.1*** no se encuentra almacenada en la base de datos de mi representada”.

Señala que “la consulta con ID ***ID.4 se trata de un número de referencia creado a efectos internos y organizativos por el anterior proveedor de servicios de atención al cliente (******EMPRESA.1***) que colaboraba con Glovoapp23, S.L. en el momento en que el usuario ******EMAIL.1*** realizó la referida consulta en fecha 1 de febrero de 2018, tal como se desprende del DOCUMENTO Nº 2 aportado por esta parte en su escrito de fecha 30 de septiembre de 2020. Cada número de referencia tenía por objeto identificar las consultas o incidentes remitidos por los usuarios de mi representada y que debían ser atendidos por dicho proveedor”.

El reclamado indica que “se realizó un cambio de software del CRM con el que gestionaba la relación con sus clientes con el fin de incrementar la seguridad y la fiabilidad de los procesos de supresión y bloqueo de datos. En este sentido, tal y como esta parte indicó en la alegación CUARTA del referido escrito de alegaciones de fecha 30 de septiembre de 2020, dicho cambio de CRM le impidió tener los datos adicionales acerca de la consulta con ID ***ID.4 de fecha 1 de febrero de 2018, por lo que esta parte no puede aportar datos adicionales más allá de la información sobre esta consulta que esta parte ya presentó en el marco de este procedimiento.

Mi representada desea resaltar que esto se debe a que el anterior proveedor de los servicios de atención al cliente (******EMPRESA.1***) tenía definido un período de conservación de los datos de los usuarios que trataba en nombre y por cuenta de sus clientes (en este caso, Glovoapp23, S.L.) de un plazo máximo de 90 días contados a partir de la finalización de la relación contractual, plazo que ya transcurrió”.

El reclamado recuerda también que “ya facilitó a esta Agencia la información de la que disponía sobre la consulta con ID ***ID.4 realizada por el usuario ******EMAIL.1***, tal como consta en su escrito de alegaciones de fecha 30 de septiembre de 2020 y que entiende esta información como completa al componerse, entre otros elementos de: número ID de referencia, vía de contacto, fecha de creación de la consulta, tipo de consulta, asunto, descripción y contenido de la consulta, conversaciones mantenidas entre el agente del servicio de atención al cliente y el usuario, cronología de la consulta e identificación del usuario ******EMAIL.1*** como usuario quien efectuó la consulta”.

Y manifiesta que “no dispone en sus bases de datos de información adicional al respecto de la consulta con ID ***ID.4 efectuada por el usuario ***EMAIL.1** que la ya facilitada tanto en el proceso de inspección iniciado por esta Agencia en el mes de febrero de 2020, como en los diferentes escritos presentados a esta Agencia incluyendo el de fecha 30 de septiembre de 2020”.

SÉPTIMO: Con fecha 21/05/2021, se notifica al reclamado la propuesta de resolución en la que se propone que, por la Directora de la Agencia Española de Protección de Datos se proceda al ARCHIVO del presente procedimiento contra la entidad, GLOVOAPP23, S.L. con CIF: B66362906, por presunta infracción del artículo 6.1 del RGPD.

OCTAVO: Tras la notificación de la propuesta de resolución, el reclamado no ha presentado ningún tipo de alegación a la propuesta de resolución.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes

HECHOS

PRIMERO: el 15 de junio de 2019 tuvo entrada en la AEPD un escrito en el que el reclamante manifestaba que en febrero de 2018 solicitó la eliminación de su cuenta de la aplicación del reclamado, a lo que le respondieron al correo electrónico con la confirmación de la recepción de su solicitud. No obstante, el 27 de mayo de 2019 recibió un correo electrónico de un pedido realizado con su cuenta, el cual no había sido realizado por él. Se puso en contacto con la empresa a través del correo electrónico y le contestaron “en un idioma extraño, con caracteres raros” solicitándole los datos de su tarjeta de crédito, que no les facilita. También contactó a través de Twitter e inicialmente le dijeron que la cuenta de su correo no existía, que el pedido en cuestión había sido cancelado y, posteriormente, ante su solicitud de acceso a la cuenta para borrar los datos bancarios, volvieron a pedirle la identificación con su DNI y tarjeta de crédito. Al enviarle los datos, le respondieron que necesitaban más datos de su tarjeta de crédito, a lo que él se opuso. Solicita que se eliminen sus datos “definitivamente de su Base de Datos, lo que ya han incumplido una vez”.

SEGUNDO: el reclamante ha aportado:

- Intercambio de correos electrónicos con fecha 1 de febrero de 2018 en el que el reclamado, desde la dirección ***support@glovohelp.***EMPRESA.1.com***, le pide al reclamante a su dirección de correo electrónico ***EMAIL.1** que responda a ese email para confirmar la baja y le indica que “Recuerda que una vez tramitada, todos tus datos serán borrados y no podrás volver a acceder al detalle de los glovos que hayas realizado”. El reclamante responde con la confirmación de la baja y se le contesta que “Tu mensaje nº (***ID.4) se está gestionando para encontrar la mejor solución posible”.
- Correo electrónico de fecha 27 de mayo de 2019, recibido en la cuenta de correo electrónico desde la que el reclamante solicitó la eliminación de su cuenta, de un “Pedido confirmado” escrito en letras de alfabeto cirílico, con número de identificación “ID: KI17LG1HM”.
- Intercambio de correos electrónicos de fecha 27 de mayo de 2019 entre el reclamante y liveops.comms@glovoapp.com en el que denuncia que se ha

hecho este pedido por otra persona, pero que los cuatro últimos dígitos de su tarjeta de crédito, que aparecen en el correo del pedido, coinciden con los de su tarjeta de crédito y que intentó conectarse a la aplicación pero le pidió confirmación al teléfono, que no coincide con su número. El reclamado "para garantizar un pago seguro" le solicita al reclamante que le envíe una copia de su DNI o pasaporte y de la tarjeta de crédito, en la que se vean únicamente el nombre del titular y los 6 primeros dígitos y 4 últimos dígitos. El reclamante responde que no quiere realizar ningún pago, que el último pedido no lo realizó él y que le suplantaron la identidad, que no puede acceder a la cuenta y que no les va a enviar sus datos bancarios porque ve una falta de seguridad importante en la aplicación y solicita que se elimine esa cuenta.

- Correos electrónicos de fecha 6 de junio de 2019 enviados por liveops.comms@glovoapp.com al reclamante en los que se indica que la cuenta ha sido bloqueada por actividades sospechosas y le solicitan copia de su DNI o pasaporte y de la tarjeta en la que se vean únicamente el nombre del titular y los 6 primeros dígitos y 4 últimos dígitos con el objeto de comprobar la identidad para revisar el estado de la cuenta. Y correo electrónico de fecha 7 de junio de 2019 enviado por liveops.comms@glovoapp.com al reclamante en el que se le solicita que vuelva a enviar la copia de su tarjeta debido a que no se pueden visualizar los 6 primeros dígitos.
- Intercambio de mensajes en Twitter desde el 27 de mayo hasta el 8 de junio de 2019 en el que el reclamante expone que se ha realizado un pedido que él no ha solicitado, que está preocupado porque los últimos dígitos de la tarjeta de crédito coinciden con la suya, que quiso acceder a su cuenta y no pudo y que el teléfono para recuperar la contraseña no es el suyo. El reclamado en un principio le contesta que el correo electrónico facilitado no corresponde a ninguna cuenta y le solicitan un número de pedido que hubiera realizado en el pasado. El reclamante les facilita el número de pedido #GJPYLGSVC de fecha 6/1/2018 y el reclamado le contesta que le consta que el pedido no solicitado ha sido cancelado sin costes y que recibirá el importe cobrado incorrectamente. El reclamante insiste en que desea eliminar sus datos de la aplicación, para lo cual quiere acceder a la misma. Para ello, el reclamado le pide que realice "una verificación que le hemos enviado a su correo". El reclamante reproduce el correo en el que le solicitan copia del DNI y copia de la tarjeta de crédito asociada a la cuenta en la que se vea su nombre y los 6 primeros dígitos y 4 últimos dígitos. El reclamante indica que envió la foto, pero el reclamado insiste en que en las imágenes adjuntadas no se pueden visualizar los primeros seis dígitos de la tarjeta y que necesitan esa información "para poder habilitar su perfil". El reclamante se niega a facilitarle estos datos por desconfianza en la seguridad de la aplicación, toda vez que en febrero había pedido eliminar la cuenta y le habían contestado que lo harían, pero meses más tarde recibe un mensaje de que se hizo un pedido desde la cuenta que había solicitado eliminar. Expone que solo quería acceder a la aplicación para eliminar su número de tarjeta de crédito y que desea eliminar esa cuenta, junto con todos sus datos personales. Finalmente, el reclamado insiste en que necesita verificar su identidad "para provecer a la devolución del importe pagado y luego podremos cancelar la cuenta". El reclamante contesta que primero le habían dicho que no existía una cuenta con su correo, luego que se ha bloqueado un pedido con su cuenta (la que le

habían dicho que no existía), más tarde le dijeron que el dinero había sido devuelto y ahora le pedían más datos para devolverle el importe que ya estaba devuelto, que estaba claro que algo fallaba o que se contradecía el reclamado y que iba a presentar denuncia ante esta Agencia.

TERCERO: en respuesta a los requerimientos de esta Agencia, así como durante la inspección presencial realizada y en su escrito de alegaciones, el reclamado ha manifestado que:

- El reclamado actuó con la debida diligencia puesto que el reclamante recibió una respuesta a su correo electrónico mediante la cual se confirmaba la recepción de su solicitud, lo cual demuestra que se trata con atención la solicitud del reclamante y le mantiene informado sobre el estado de su solicitud.

- Respecto a las medidas adoptadas para evitar incidencias similares: el reclamado enumera la congelación y pseudonimización de los datos del reclamante, de acuerdo con el citado art. 17.3.e); la cancelación del pedido supuestamente fraudulento, pese a que éste pudo deberse a un posible hackeo no atribuible al reclamado; y que se procedió a señalar y bloquear el perfil completo del usuario, con el fin de evitar posibles fraudes que pudieran afectarle. Como acciones de mejora desde 2018, el reclamado enumera:

1. Cambio del software de CRM con el que se gestiona la relación con los clientes, pasado de la aplicación ******EMPRESA.1*** a ******EMPRESA.2***.

2. Mantenimiento y mejora de la plataforma que previene las acciones de fraude y bloquea los intentos que respondan a un patrón sospechoso.

3. Mantenimiento y mejora del doble factor de autenticación, eliminando el riesgo relativo a las cuentas inactivas cuyo teléfono móvil no fue verificado y el doble factor no fue activado.

4. Seudonimización de los datos bloqueados por sospecha de fraude.

5. Aplicación de las medidas de verificación de usuarios con dos cuentas a raíz del caso ******CASO.1***, que también llegó a la AEPD."

- A finales del año 2018, se incluyó una medida de seguridad en su aplicación que consistía en que, siempre que un usuario se autentique desde un nuevo dispositivo, se le envía un código de verificación al teléfono móvil que hubo introducido durante el proceso de alta. Este proceso ya se utilizaba durante el proceso de alta para verificar que el número de teléfono introducido estaba en posesión del usuario.

- Tras la realización de cada pedido, se verifica automáticamente si la operación corresponde con algún patrón de intento de fraude y, en el caso de ser así, aparece una alerta para que un empleado del reclamado bloquee la cuenta manualmente y alguien del departamento de fraude le solicite más información al usuario vía correo electrónico con el objeto de levantar el bloqueo de la cuenta. Mientras dura el bloqueo de la cuenta, si el usuario intenta acceder a su cuenta, se le muestra un mensaje de

aviso indicando que contacte con atención al cliente; este mensaje se observa en el ejemplo de captura de pantalla aportada durante la inspección.

- La cuenta de usuario con la que supuestamente se hizo el pedido el 27 de mayo de 2019 tiene como fecha de creación en los sistemas de información del reclamado el 1 de junio de 2018, y como fecha de borrado el 10 de septiembre de 2019. Esto se desprende las capturas de pantalla realizadas durante la inspección en la base de datos y en la plataforma de administración del investigado sobre el pedido ***KI17LG1HM*** y los datos del cliente ***ID.4, asociados a ese pedido.

- Los hechos ocurridos en relación con la cuenta del usuario reclamante coinciden plenamente con el patrón de actuación habitual de los ciberdelincuentes que utilizan los datos comercializados en el mercado negro de países de la Europa del Este como Ucrania para suplantar la identidad de sus víctimas y realizar compras fraudulentas. En este caso concreto, veremos que el ciberataque se realiza desde Ucrania y que aprovecha la actuación negligente del reclamante, al utilizar reiteradamente la misma clave en distintos servicios que fueron afectados por una brecha de seguridad que dejó expuestas sus credenciales.

- El sitio web haveibeenpwned.com ofrece un servicio gratuito que permite a cualquier usuario comprobar si su dirección de correo electrónico figura en estas listas, y por lo tanto, si sus claves han quedado comprometidas y debe cambiarlas de inmediato. Si introducimos la dirección ******EMAIL.1*** en esta base de datos, se comprueba que las credenciales del reclamante han quedado expuestas en cinco brechas de seguridad y dos intentos o indicios de ataque.

- La investigación también demostró que el reclamante tenía abierta otra cuenta en Glovo con la dirección ******EMAIL.2***, domicilio de entrega y tarjeta de crédito (dígitos iniciales y finales coincidentes).

- Los datos del reclamante inicialmente expuestos en estas listas se limitaban a la dirección de correo electrónico y a la clave de acceso, y, en las últimas versiones de 2019 los datos del reclamante habían sido enriquecidos con muchos más datos, que incluyen:
1. Ubicación geográfica
2. Datos de empleo
3. Números de teléfono
4. Perfiles en redes sociales
5. Tarjetas de crédito”

- El reclamante es un exponente de escasa diligencia en la gestión y custodia de sus credenciales, ya que su historial de claves expuestas en brechas de seguridad se inicia en 2008 y llega hasta 2019, y el éxito de la suplantación de identidad confirma que durante todo este tiempo el reclamante no ha cambiado las claves de acceso reiteradamente comprometidas. En los Términos y Condiciones que regulan el servicio, disponibles en https://glovoapp.com/es/legal/terms, Glovo advierte a los usuarios de su responsabilidad con respecto a la elección de sus contraseñas y al usar la app de Glovo el usuario acepta expresamente estas obligaciones: “Cláusula 17. - Los Usuarios son completamente responsables del acceso y correcto uso de su perfil y demás contenidos de la Plataforma con sujeción a la legalidad vigente, sea nacional o

internacional del País desde el que hace uso de la Plataforma, así como a los principios de buena fe, a la moral, buenas costumbres y orden público. Y específicamente, adquiere el compromiso de observar diligentemente las presentes Condiciones Generales de Uso.

Los Usuarios son responsables de consignar correctamente nombres de usuario y contraseñas individuales, no transferibles y lo suficientemente complejas, así como no usar el mismo nombre de usuario y contraseña que en otras plataformas, todo ello con la finalidad de proteger su cuenta del uso fraudulento por parte de terceros ajenos a la plataforma. (...)"

- El cambio de la aplicación de CRM destinada a recopilación de todas las acciones y transacciones de los clientes le impide al reclamado tener los logs con los detalles de las operaciones realizadas en 2018.

- El reclamado realizó la supresión y el bloqueo de los datos del reclamante de forma correcta y comunicó la supresión al reclamante, para lo cual aporta como DOCUMENTO 2 la captura de la pantalla extraída de la copia de seguridad, en la que aparece esta confirmación.

En este Documento 2, adjunta una tabla en la que se puede observar, entre otra, la siguiente información:

id	subject	submitter	comment	Message created at
***ID.4	Eliminación de cuenta	{'id': 116472211014, 'url': 'https://glovoservice.***EMPRESA.1*.com/api/v2/users/116472211014.json', 'name': '***A.A.A.***', 'email': '****EMAIL.1***', 'created_at': '2018-01-	Hola, he estado buscando tanto en la aplicación cómo en la página web, y no he encontrado en ningún sitio forma de eliminar la cuenta. Entiendo que esto debería ser posible de una forma sencilla (aunque esté escondido), y si no puede ser desde la App que fuese desde la página web. ¿Pueden decirme cómo debo proceder al respecto?	2018-02-01T19:39:34.000Z
***ID.4	Eliminación de cuenta	{'id': 116472211014, 'url': 'https://glovoservice.***EMPRESA.1*.com/api/v2/users/116472211014.json', 'name': '***A.A.A.***', 'email': '****EMAIL.1'***, 'created_at': '2018-01-	¡Hola ***A.A.A.***! Las despedidas siempre son duras, ¡no queremos que te vayas! :(, aunque nos gustaría saber el motivo por el cual has decidido irte, ¡nos importa tu opinión! Si ya te lo has pensado bien y quieres eliminar tu cuenta, responde a este email confirmando la baja y gestionaremos tu petición a la mayor brevedad posible. Recuerda que una vez tramitada, todos tus datos serán borrados y no podrás volver a acceder al detalle de los	2018-02-01T19:40:28.000Z
***ID.4	Eliminación de cuenta	{'id': 116472211014, 'url': 'https://glovoservice.***EMPRESA.*	Confirmo la eliminación, gracias Un saludo El 1 feb 2018, a las 20:40, Glovo <support@glovohelp.***EMPRESA.1.com> escribió:	2018-02-01T19:44:18.000Z

		1.com/ api/v2/users/116 472211014.json', 'name': 'A.A.A.', 'email': ******EMAIL.1***', 'created_at':		
***ID.4	Eliminación de cuenta	{'id': 116472211014, 'url': 'https://glovoservi ce.******EMPRESA. 1***.com/ api/v2/users/116 472211014.json', 'name': '***A.A.A.***', 'email': ******EMAIL.1***', 'created_at':	solved en ***ID.4	2018-02-01T19:49:22.000Z
1511051	Eliminación de cuenta	360237355414, 'url': 'https://glovoservi ce.******EMPRESA. 1***.com/ api/v2/users/360 237355414.json', 'name': '***A.A.A.***', 'email':	Quiero eliminar mi cuenta de Glovo ---------- Enviado desde: https://glovoapp.com/es/contact	2018-02-01T19:45:30.000Z
1511051	Eliminación de cuenta	{'id': 360237355414, 'url': 'https://glovoservi ce.******EMPRESA. 1***.com/ api/v2/users/360 237355414.json', 'name': '***A.A.A.***', 'email': '******EMAIL.3***	¡Hola ***A.A.A.***! Las despedidas siempre son duras, ¡no queremos que te vayas! :(, aunque nos gustaría saber el motivo por el cual has decidido irte, ¡nos importa tu opinión! Si ya te lo has pensado bien y quieres eliminar tu cuenta, responde a este email confirmando la baja y gestionaremos tu petición a la mayor brevedad posible.	2018-02-01T19:47:18.000Z
1511051	Eliminación de cuenta	360237355414, 'url': 'https://glovoservi ce.******EMPRESA. 1***.com/ api/v2/users/360 237355414.json', 'name': '***A.A.A.***', 'email':	El 1 feb 2018, a las 20:47, Glovo <support@glovohelp.***EMPRESA.1.com> escribió:	2018-02-01T19:47:56.000Z
1511051	Eliminación de cuenta	{'id': 360237355414, 'url': 'https://glovoservi ce.******EMPRESA. 1***.com/ api/v2/users/360 237355414.json', 'name': '***A.A.A.***', 'email': '******EMAIL.3***	¡Hola ***A.A.A.***! Ya no hay vuelta atrás :(Te confirmamos que hemos eliminado tu cuenta de usuario de nuestra base de datos. Tal y como te comentamos, ya no podrás acceder a tu perfil ni al detalle de tus pedidos anteriores. La baja del envío de la newsletter a tu correo electrónico se hará efectiva en aproximadamente unas 48 horas hábiles	2018-02-01T19:48:43.000Z
***ID.5	Eliminación de cuenta	{'id': 116018503873,	Quiero borrar mi cuenta, vinculada a través	2018-02-01T19:46:2

		'url': 'https://glovoservice.***EMPRESA.1*.com/api/v2/users/116018503873.json', 'name': ***'A.A.A.***', 'email': ***'***EMAIL.2***	de Facebook, Gracias un saludo ---------- Enviado desde: https://glovoapp.com/es/contact	3.000Z
***ID.5	Eliminación de cuenta	{'id': 116018503873, 'url': 'https://glovoservice.***EMPRESA.1*.com/api/v2/users/116018503873.json', 'name': ***'A.A.A.'***, 'email': ***'***EMAIL.2***	¡Hola ***A.A.A.***! Las despedidas siempre son duras, ¡no queremos que te vayas! :(, aunque nos gustaría saber el motivo por el cual has decidido irte, ¡nos importa tu opinión! Si ya te lo has pensado bien y quieres eliminar tu cuenta, responde a este email confirmando la baja y gestionaremos tu petición a la mayor brevedad posible. Recuerda que una vez tramitada, todos tus datos serán borrados y no podrás volver a acceder al detalle de los	2018-02-01T19:48:10.000Z
***ID.5	Eliminación de cuenta	{'id': 116018503873, 'url': 'https://glovoservice.***EMPRESA.1*.com/api/v2/users/116018503873.json', 'name': ***'A.A.A.***', 'email': ***'***EMAIL.2***	Confirmo la eliminación de la cuenta, un saludo El 1 feb 2018, a las 20:48, Glovo <support@glovohelp.***EMPRESA.1.com> escribió:	2018-02-01T19:48:48.000Z
***ID.5	Eliminación de cuenta	{'id': 116018503873, 'url': 'https://glovoservice.***EMPRESA.1*.com/api/v2/users/116018503873.json', 'name': ***'A.A.A.***, 'email': ***'***EMAIL.2***	¡Hola ***A.A.A.***! Ya no hay vuelta atrás :(Te confirmamos que hemos eliminado tu cuenta de usuario de nuestra base de datos. Tal y como te comentamos, ya no podrás acceder a tu perfil ni al detalle de tus pedidos anteriores. La baja del envío de la newsletter a tu correo electrónico se hará efectiva en aproximadamente unas 48 horas hábiles. Si tienes cualquier otra consulta al respecto, no dudes en contactarnos respondiendo a este mismo email.	2018-02-01T19:52:54.000Z

- El cambio de la aplicación de CRM destinada a recopilación de todas las acciones y transacciones de los clientes impide al reclamado tener los logs con los detalles de las operaciones realizadas en 2018, por lo que su investigación se ha centrado en verificar o refutar las cuatro hipótesis de trabajo que desarrolla en su escrito de alegaciones.

- Una primera hipótesis: que el ciberatacante utilizó las credenciales del reclamante, desbloqueó y restauró la cuenta anterior. Indica el reclamado que para haber realizado el pedido fraudulento, el ciberdelincuente debería haber conseguido permisos de administrador y realizado siguientes pasos descritos y haber sorteado todos los obstáculos establecidos para impedirlo:

Paso	Requisito obligatorio	Obstáculos
Acceso a la cuenta	Reconocimiento de las credenciales del reclamante	Si el ciberdelincuente hubiese utilizado la dirección de correo electrónico y la clave de acceso del reclamante, el sistema no las habría reconocido, ya que la cuenta ya no existía y los datos estaban suprimidos, bloqueados y excluidos del tratamiento.
Verificación mediante doble factor de autenticación	Envío de SMS al móvil y aceptación del usuario	Si la cuenta del reclamante no se hubiese deshabilitado, el intento de acceso del ciberdelincuente habría sido neutralizado por el doble factor, al no haber recibido el ciberdelincuente el SMS con el código de acceso. Sin embargo, la investigación ha encontrado indicios de que el reclamante pudo no verificar el número de móvil, por lo que no se activado el doble factor. Ello sería compatible con la escasa diligencia del reclamante en materia de seguridad informática.
Restauración de la cuenta	Acceso a los datos, desbloqueo de los datos y conversión de la cuenta en una cuenta operativa	Para realizar estas acciones el atacante debería haber conseguido permisos de administrador del sistema y no consta en los logs del sistema ningún ataque de este nivel. Además, sería absolutamente desproporcionado organizar un ataque tan potente para realizar un pedido minúsculo.
Modificación del domicilio	Modificación de datos que estaban bloqueados y trazabilidad de la modificación	No consta en el sistema ninguna solicitud de modificación del domicilio de entrega. El ciberdelincuente no podía acceder a los datos ni modificarlos ya que estaban bloqueados.
Pago del pedido	Acceso al medio de pago	Glovo no conserva el número completo de la tarjeta de crédito y la investigación ha demostrado que todos los datos estaban bloqueados.

También señala que sería absolutamente desproporcionado organizar un ataque tan potente para realizar un pedido minúsculo. Por todo ello el reclamado concluye que esta primera hipótesis debe ser rechazada.

- Una segunda hipótesis: el reclamante nunca verificó su número de teléfono móvil y el doble factor de autenticación quedó sin activar. Indica el reclamado que es posible que una cuenta que se quede inactiva durante unos meses (dormant account), pase a un modo de semibloqueo y no reaccione a la orden de supresión). El reclamado alega que “una cuenta no verificada y sin el doble factor activado coincide con un patrón de intento de fraude y por tanto se bloquea la cuenta. Este bloqueo sería distinto del bloqueo post supresión, ya que en los intentos de fraude los datos bloqueados siguen en la base de datos principal porque deben ser consultados por el equipo antifraude para prevenir nuevos intentos de fraude. Sin embargo, esta hipótesis no encaja con el hecho de que mi representada verificó y confirmó en febrero de 2018 que la cuenta había sido correctamente suprimida”.

- Una tercera hipótesis: el ciberatacante creó una nueva cuenta utilizando la dirección de correo electrónico y los datos de la tarjeta de crédito del reclamante, obtenidos en el mercado negro. El reclamado alega que “La AEPD constató, en el transcurso de la inspección en Glovo, y lo considera como un hecho probado, que el pedido fraudulento

se realizó con una cuenta que había sido creada el 1 de junio de 2018. Ello se repite varias veces en el acuerdo de inicio de procedimiento sancionador y en las actas de la inspección. Este dato es muy importante, porque demuestra que la cuenta con la que se realizó el pedido fraudulento no fue la misma que creó el reclamante. ES UNA CUENTA DISTINTA.

La primera cuenta tenía el ID ***ID.1 y la segunda el ID ***ID.3.

Además, la primera cuenta utilizó una tarjeta MASTERCARD y la segunda una tarjeta VISA.

Recordemos que los hechos probados se inician en febrero de 2018, cuando el reclamante solicita la eliminación de su cuenta y la supresión de sus datos.

Sin embargo, las comprobaciones realizadas por la AEPD demuestran que la cuenta utilizada para realizar el pedido fraudulento fue creada CUATRO MESES DESPUÉS de que el reclamante solicitase la cancelación de su cuenta y Glovo procediese a suprimir y bloquear los datos.

Entendemos que fue el ciberdelincuente el que abrió esa cuenta en junio de 2018 con los datos que había obtenido en las listas de direcciones de correo electrónico que se venden en internet y en el mercado negro.

Ello acreditaría que la supresión de la cuenta y el bloqueo de los datos se realizó correctamente, ya que, de lo contrario el ciberdelincuente no habría podido utilizar la misma dirección de correo electrónico".

El reclamado indica que, para que esta hipótesis fuese factible, deberían haberse cumplido los siguientes requisitos:

Paso	Requisito obligatorio	Obstáculos
Acceso a la cuenta	Apertura de nueva cuenta	No existen obstáculos para la creación de una nueva cuenta porque la dirección de correo electrónico del reclamante había sido suprimida y no se producía una duplicidad de cuenta.
Verificación mediante doble factor de autenticación	Envío de SMS al móvil y aceptación del usuario	El ciberdelincuente utilizó su propio móvil para instalar la aplicación y la nueva cuenta. Recibió el SMS en él y la cuenta quedó verificada. **Esta verificación está acreditada y se produjo el 27 de mayo de 2019 a las 11:14 pm CEST, de acuerdo con el log del sistema.** Adjuntamos como DOCUMENTO TRES el log de verificaciones. Por eso el reclamante no recibió un SMS de verificación y por eso el reclamante vio que el número de móvil de la cuenta no coincidía con el suyo.
Modificación del domicilio	Modificación de datos que estaban bloqueados y trazabilidad de la modificación	Al ser una cuenta nueva, el ciberdelincuente puso el domicilio que consideró oportuno para la entrega.
Pago del pedido	Acceso al medio de pago	El ciberdelincuente obtuvo los datos de la tarjeta asociada a la dirección de correo electrónico del reclamante en el mercado negro.

El reclamado también alega que es notorio y ampliamente conocido que, en el mercado negro de la Internet profunda, se pueden adquirir datos de tarjetas de crédito que han quedado expuestas y que se pueden adquirir listas de cuentas con tarjetas de crédito no anuladas tras una brecha de seguridad. Y que el reclamado defiende que el ciberatacante obtuvo los datos de la tarjeta de crédito asociada a la dirección de correo del reclamante en una de estas listas.

Para ello, resalta dos hechos:

1. El reclamante sufrió una brecha de seguridad en su cuenta de Dropbox, donde podía conservar los datos de su tarjeta de crédito.

2. Los datos del reclamante figuraban en la lista enriquecida que fue descubierta en 2019, pero que contenía datos de una antigüedad superior, que habían sido enriquecidos con aportaciones de otros ciberdelincuentes.

Señala el reclamado que Ucrania es también un país históricamente relacionado con el phishing, por lo que la facilidad para acceder a datos de tarjetas de crédito es muy superior a la de otros países. Y que, por todo ello, considera que la opción más probable es que el ciberdelincuente utilizase los datos de la tarjeta de crédito del reclamante para realizar el pedido fraudulento, dado que las otras opciones son mucho menos probables.

El reclamado destaca también que el cargo relativo al pedido fraudulento nunca llegó a realizarse, ya que fue Glovo la que detectó un patrón sospechoso y bloqueó el pago, por lo que en ningún momento se causaron perjuicios al reclamante.

Finalmente, el reclamado indica que, de acuerdo con las evidencias que constan en el procedimiento, obtenidas durante la inspección en las oficinas de Glovo, y aportadas por el reclamante y por el reclamado, la cronología de los hechos es la siguiente:

Año	Descubrimiento de las claves de acceso del reclamante en listas de claves
2012	Las claves de acceso de la cuenta del reclamante en Dropbox quedan expuestas
2016	Las claves de acceso de la cuenta del reclamante en LinkedIn quedan expuestas
2016	Las claves de acceso del reclamante aparecen en la lista Exploit.In
2019	Las claves de acceso del reclamante aparecen en la lista Collection 1#
2019	Las claves de acceso y otros datos del reclamante aparecen en una lista enriquecida

Año	Hechos
02/2018	El reclamante solicita la supresión de su cuenta y de sus datos
02/2018	Glovo suprime la cuenta y los datos y conserva una copia bloqueada en el datawarehouse
06/2018	El ciberdelincuente crea una cuenta en Glovo con los datos del reclamante
05/2019	El ciberdelincuente realiza un pedido fraudulento
05/2019	El reclamante recibe un mensaje de confirmación del pedido y lo comunica a Glovo

Y alega que “Esta cronología encaja perfectamente con los hechos probados y demuestra que mi representada actuó diligentemente y sin infringir la normativa de protección de datos.

La simple posibilidad de que los hechos se hayan producido de esta manera y no como la Agencia sostiene, pero no acredita, permite a mi representada acogerse al principio de presunción de inocencia administrativa y adopta como hipótesis más verosímil la relativa a la creación de una nueva cuenta por parte del atacante, que en ningún momento ha sido contradicha por la Agencia”.

- Una cuarta hipótesis: el reclamante abrió una nueva cuenta después de la supresión de la anterior. El reclamado indica que esta hipótesis no sería descabellada, ya que, además de la cuenta de Glovo ******EMAIL.1***, el reclamante disponía de la cuenta ******EMAIL.2***, de la cual había olvidado su existencia, o al menos solo ejercitó el derecho de supresión en relación a una de ellas.

“Por ello, y a pesar de que los logs del sistema no conservan los datos de junio de 2018 para comprobar la dirección IP desde la que se produjo la apertura de esta nueva cuenta, es perfectamente factible que el reclamante abriese una nueva cuenta el 1 de junio de 2018 y después se olvidase de que la había abierto.

Esta hipótesis encajaría plenamente con la supresión inicial de los datos y la posterior suplantación de identidad por parte del ciberdelincuente, ya que los datos de la segunda cuenta abierta por el reclamante no habrían sido suprimidos.

Recordemos que los ID de las dos cuentas eran diferentes y las tarjetas de crédito también.

La cronología de los hechos relativa a esta hipótesis sería la siguiente:

Año	Hechos
02/2018	El reclamante solicita la supresión de su cuenta y de sus datos
02/2018	Glovo suprime la cuenta y los datos y conserva una copia bloqueada en el datawarehouse
06/2018	El reclamante crea una nueva cuenta
05/2019	El ciberdelincuente accede a la nueva cuenta con los datos del reclamante
05/2019	El ciberdelincuente realiza un pedido fraudulento
05/2019	El reclamante recibe un mensaje de confirmación del pedido y lo comunica a Glovo

Esta cronología también encaja con los hechos probados y demuestra que mi representada actuó diligentemente y sin infringir la normativa de protección de datos.

También en esta hipótesis, la simple posibilidad de que los hechos se hayan producido de esta manera y no como la Agencia sostiene, pero no acredita, permite a mi representada acogerse al principio de presunción de inocencia administrativa y adopta como hipótesis más verosímil la relativa a la creación de una nueva cuenta por parte del reclamante, que en ningún momento ha sido contradicha por la Agencia".

- En cada una de las hipótesis de trabajo barajadas por el reclamado, se actuó con sujeción a la ley y en ningún caso mantuvo los datos del reclamante accesibles a personas diferentes de las autorizadas para acceder a los datos bloqueados en el datawarehouse.

Diferentes firmas de reconocido prestigio han emitido, con carácter previo al cierre de cada una de las rondas de financiación, informes de situación sobre el cumplimiento normativo de la compañía (Due Diligence). El reclamado ha cumplido puntualmente las recomendaciones contenidas en dichos informes con el fin de asegurar la protección de los derechos y libertades de los interesados.

En ninguno de estos informes se ha indicado que el reclamado disponga de unas medidas de seguridad insuficientes en relación con el proceso de autenticación de los usuarios.

- En relación con el carácter continuado de la infracción, se ha acreditado que la cronología de los hechos sostenida por la AEPD no se corresponde con la realidad y que no se ha producido infracción alguna.

- En relación con la cuantía de los usuarios, esta es errónea, ya que la cifra es muy inferior y a los efectos de este procedimiento deben tenerse en cuenta únicamente las cuentas activas. Si fuese cierto que trata los datos de más de 7 millones de clientes activos, sería un gran éxito haber tenido un único incidente de estas características, ya que por simple probabilidad estadística, los errores humanos o informáticos arrojan cifras de incidentes muy superiores.

- Ha actuado en todo momento de buena fe, empleando su mayor compromiso, y sin nunca poner en peligro los derechos y libertades de los interesados. No existe, pues, una clara "intencionalidad" en incumplir con la normativa vigente ya que realizó todas las acciones necesarias y debidas para el cumplimiento de la normativa y ha ajustado prudentemente su actuación a la ley.

- La cuenta de usuario de Glovo asociada a la dirección de correo electrónico ***EMAIL.1**, desde la que se realizó el pedido fraudulento, corresponde al ID ***ID.4.

- La consulta con ID ***ID.4 se trata de un número de referencia creado a efectos internos y organizativos por el anterior proveedor de servicios de atención al cliente (***EMPRESA.1**) que colaboraba con Glovoapp23, S.L. en el momento en que el usuario ***EMAIL.1** realizó la referida consulta en fecha 1 de febrero de 2018, tal como se desprende del DOCUMENTO Nº 2 aportado en su escrito de fecha 30 de septiembre de 2020. Cada número de referencia tenía por objeto identificar las consultas o incidentes remitidos por los usuarios del reclamado y que debían ser atendidos por dicho proveedor.

- Se realizó un cambio de software del CRM con el que gestionaba la relación con sus clientes con el fin de incrementar la seguridad y la fiabilidad de los procesos de supresión y bloqueo de datos. En este sentido, dicho cambio de CRM le impidió tener los datos adicionales acerca de la consulta con ID ***ID.4 de fecha 1 de febrero de 2018. Esto se debe a que el anterior proveedor de los servicios de atención al cliente (***EMPRESA.1**) tenía definido un período de conservación de los datos de los usuarios que trataba en nombre y por cuenta de sus clientes (en este caso, Glovoapp23, S.L.) de un plazo máximo de 90 días contados a partir de la finalización de la relación contractual, plazo que ya transcurrió.

- Ya facilitó a esta Agencia la información de la que disponía sobre la consulta con ID ***ID.4 realizada por el usuario ***EMAIL.1**, tal como consta en su escrito de alegaciones de fecha 30 de septiembre de 2020 y que entiende esta información como completa al componerse, entre otros elementos de: número ID de referencia, vía de contacto, fecha de creación de la consulta, tipo de consulta, asunto, descripción y contenido de la consulta, conversaciones mantenidas entre el agente del servicio de atención al cliente y el usuario, cronología de la consulta e identificación del usuario ***EMAIL.1** como usuario quien efectuó la consulta".

CUARTO: el reclamado es una gran empresa en su sector de negocio y el desarrollo de la actividad empresarial que desempeña requiere un tratamiento continuo de datos personales.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el art. 58.2 del RGPD y en los art. 47 y 48.1 de LOPDGDD.

II

En el presente caso, el reclamante reclama que había solicitado la supresión de su cuenta de Glovo asociada a su correo electrónico ***EMAIL.1** en febrero de 2018 y el reclamado le había confirmado que dicha solicitud se estaba tramitando. No obstante, el 19 de mayo de 2019 recibió en esta dirección de correo una confirmación de un pedido realizado que él no había solicitado, por lo que entendía que la supresión de su cuenta por él solicitada no había sido atendida debidamente y la cuenta en cuestión había permanecido activa.

Al respecto, el artículo 17 del RGPD “Derecho de supresión (“el derecho al olvido)” establece que:

“1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1 (…)”.

Por su parte, el artículo 12 del RGPD *“Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado”* dispone:

“(…) 2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.

3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, sin dilación indebida y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

4. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales. (…)”

En el presente caso, de no haber dado curso debidamente a la solicitud de supresión de la cuenta se estarían tratando los datos personales del reclamante sin tener base jurídica que legitime tal tratamiento.

En este sentido, el artículo 5 del RGPD "*Principios relativos al tratamiento*" establece que:

"1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»); (…)

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)".

Y el artículo 6 del RGPD "*Licitud del tratamiento*" dispone:

"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones. (…)"

III

En el presente caso, el reclamante tenía una cuenta de usuario de Glovo asociada a su correo electrónico ******EMAIL.1***. Según el DOCUMENTO 2 que acompaña al escrito de alegaciones del reclamado, con fecha 1 de febrero de 2018, a las 19:39hs el reclamante solicitó al reclamado la supresión de esta cuenta, mediante consulta ID

ID.4. El reclamado, a través de su proveedor ***EMPRESA.1 le habría respondido a las 19:40hs “¡Hola ***A.A.A.***! Las despedidas siempre son duras, ¡no queremos que te vayas! :(, aunque nos gustaría saber el motivo por el cual has decidido irte, ¡nos importa tu opinión! Si ya te lo has pensado bien y quieres eliminar tu cuenta, responde a este email confirmando la baja y gestionaremos tu petición a la mayor brevedad posible. Recuerda que una vez tramitada, todos tus datos serán borrados y no podrás volver a acceder al detalle de los”. A las 19:44hs el reclamante habría contestado “Confirmo la eliminación, gracias Un saludo”. A este mensaje, el reclamante no habría recibido respuesta posterior. No obstante, aparece el mensaje “solved en ***ID.4” a las 19:49hs en los sistemas de ***EMPRESA.1***. Cabe señalar que no fue posible obtener el número de identificación de la cuenta de usuario asociado a la consulta ID ***ID.4, dado que, según manifiesta el reclamado en sus alegaciones, el anterior proveedor de servicio de atención al cliente del reclamado (***EMPRESA.1***) tenía definido un período de conservación de los datos de los usuarios que trataba en nombre y por cuenta de sus clientes (en este caso, el reclamado) de un plazo máximo de 90 días contados a partir de la finalización de la relación contractual, plazo que ya transcurrió. Tampoco se ha podido determinar la fecha de creación de esta cuenta.

El 19 de mayo de 2019 se realizó un pedido #GJPYLGSVC, con ID: ***ID.6, desde la cuenta del cliente ID ***ID.4, asociada al correo electrónico ***EMAIL.1***. El reclamante se comunicó con el reclamado, el cual canceló el pedido en cuestión sin generar gasto alguno para el reclamante y procedió a marcar esa cuenta como fraudulenta. Según consta de los hechos reseñados, esta cuenta ID ***ID.4 fue creada el 1 de junio de 2018 y borrada el 10 de septiembre de 2019.

Además de tener una cuenta asociada al correo ***EMAIL.1***, el reclamante tenía una cuenta asociada a su correo electrónico ***EMAIL.2***, con ID ***ID.1, vinculada a su cuenta de Facebook. Según consta del DOCUMENTO 2 que acompaña al escrito de alegaciones del reclamado, el día 1 de febrero de 2018 a las 19:46hs el reclamante solicitó el borrado de esta cuenta. El reclamado, a través de su proveedor ***EMPRESA.1***, le contestó a las 19:48hs “¡Hola ***A.A.A.***! Las despedidas siempre son duras, ¡no queremos que te vayas! :(, aunque nos gustaría saber el motivo por el cual has decidido irte, ¡nos importa tu opinión! Si ya te lo has pensado bien y quieres eliminar tu cuenta, responde a este email confirmando la baja y gestionaremos tu petición a la mayor brevedad posible. Recuerda que una vez tramitada, todos tus datos serán borrados y no podrás volver a acceder al detalle de los”. El reclamante, a las 19:48hs, respondió con el siguiente mensaje: “Confirmo la eliminación de la cuenta, un saludo”. A las 19:52hs el reclamado le contestó: “¡Hola ***A.A.A.***! Ya no hay vuelta atrás :(Te confirmamos que hemos eliminado tu cuenta de usuario de nuestra base de datos. Tal y como te comentamos, ya no podrás acceder a tu perfil ni al detalle de tus pedidos anteriores. La baja del envío de la newsletter a tu correo electrónico se hará efectiva en aproximadamente unas 48 horas hábiles. Si tienes cualquier otra consulta al respecto, no dudes en contactarnos respondiendo a este mismo email.”

Si bien se aprecia que en la consulta con ID ***ID.5, en la que se solicita la supresión de la cuenta ID ***ID.1 asociada al correo electrónico ***EMAIL.2***, una vez confirmada la supresión por parte del reclamante se le contesta confirmando que se ha producido esa eliminación de la base de datos del reclamado, esto no es así en la consulta con ID ***ID.4, en la que el reclamante solicitó la supresión de su cuenta de usuario asociado al correo electrónico ***EMAIL.1***. En esta última, en el DOCUMENTO 2 que

se acompaña al escrito de alegaciones de fecha 30 de septiembre de 2020, solo se puede observar un mensaje que dice “solved en ***ID.4”, sin más detalle. Por tanto, no ha quedado acreditado en el expediente que tal supresión se hubiera realizado correctamente ni que no se hubiera realizado.

Analizando las hipótesis planteadas por el reclamado, tampoco ha quedado acreditado que alguna de esas hipótesis hubiera ocurrido realmente.

Es plausible que un ciberatacante hubiera conseguido y utilizado las credenciales del reclamante, ya que si la cuenta no hubiera sido suprimida debidamente, el sistema las habría reconocido y podría haber accedido y realizar el pedido en cuestión. Alega el reclamado que “si la cuenta del reclamado no se hubiese deshabilitado, el intento de acceso del ciberdelincuente habría sido neutralizado por el doble factor, al no haber recibido el ciberdelincuente el SMS con el código de acceso”. Y añade que “la investigación ha encontrado indicios de que el reclamante pudo no verificar el número de móvil, por lo que no se activado el doble factor. Ello sería compatible con la escasa diligencia del reclamante en materia de seguridad informática”. En el DOCUMENTO 3 que acompaña a su escrito de alegaciones, se aporta el log de verificaciones en el que se puede observar que se verificó el dispositivo móvil de la cuenta utilizada para realizar el pedido fraudulento el día 27 de mayo de 2019 a las 11:14pm CEST. Es decir, se verificó el dispositivo móvil con posterioridad a la creación de la cuenta ID ***ID.4 y previo a la realización del pedido no solicitado por el reclamante. Por tanto, no parecería que el doble factor hubiera impedido el acceso a la cuenta.

Parece menos plausible (aunque no imposible) que el reclamante nunca hubiera verificado su número de teléfono móvil y que el doble factor de autenticación hubiera quedado sin activar (segunda hipótesis) y que aún así la cuenta pudiera haberse utilizado para realizar el pedido fraudulento. En las alegaciones se explica que es posible que una cuenta que se quede inactiva durante unos meses (dormant account), pase a un modo de semibloqueo y no reaccione a la orden de supresión. No obstante, en las alegaciones también se explica que una cuenta no verificada y sin el doble factor activado coincide con un patrón de intento de fraude y por tanto se bloquea la cuenta. Es decir, que si no se hubiera eliminado debidamente la cuenta del reclamante y éste no hubiera activado el doble factor de autenticación, igualmente el sistema lo había marcado como un patrón de intento de fraude y la cuenta se hubiera bloqueado.

Por su parte, también resulta plausible que un ciberatacante hubiera creado una nueva cuenta utilizando la dirección de correo electrónico y los datos de la tarjeta de crédito del reclamante obtenidos en el mercado negro (tercera hipótesis). Esta es la hipótesis defendida por el reclamado por las siguientes razones:

- La cuenta desde la que se realizó el pedido fraudulento tiene fecha de creación 1 de junio de 2018.

- Existe una primera cuenta con ID ***ID.1, con una tarjeta MASTERCARD, y una segunda cuenta con ID ***ID.3, con una tarjeta VISA.

- No existen obstáculos para la creación de una nueva cuenta porque la dirección de correo electrónico del reclamante había sido suprimida y no se producía una duplicidad de cuenta.

- El ciberdelincuente utilizó su propio móvil para instalar la aplicación y la nueva cuenta. Recibió el SMS en él y la cuenta quedó verificada. Esta verificación está acreditada y se produjo el 27 de mayo de 2019 a las 11:14 pm CEST, de acuerdo con el log del sistema. Adjuntamos como DOCUMENTO TRES el log de verificaciones. Por eso el reclamante no recibió un SMS de verificación y por eso el reclamante vio que el número de móvil de la cuenta no coincidía con el suyo.

- Al ser una cuenta nueva, el ciberdelincuente puso el domicilio que consideró oportuno para la entrega

- El ciberdelincuente obtuvo los datos de la tarjeta asociada a la dirección de correo electrónico del reclamante en el mercado negro.

Al respecto, cabe señalar que la primera cuenta con ID ***ID.1 está asociada a la dirección de correo electrónico ******EMAIL.2***. Por tanto, no tiene relación con la cuenta objeto del pedido fraudulento, asociada a la dirección de correo electrónico ******EMAIL.1***. Aunque el reclamado tuviera varias cuentas, se trata de cuentas independientes.

La segunda cuenta, con ID ***ID.3, no ha quedado establecido que perteneciera al reclamante ni tampoco a qué dirección de correo electrónico estaba asociada. La cuenta que sí ha quedado establecida como asociada a la dirección de correo electrónico ******EMAIL.1*** y desde la que se realizó el pedido fraudulento es la cuenta ID ***ID.4. Tampoco ha podido establecerse el ID de la cuenta que inicialmente había creado el reclamante con esta dirección de correo electrónico.

Tampoco ha quedado acreditado que el ciberdelincuente que supuestamente realizó el pedido fraudulento hubiera utilizado su propio móvil y hubiera verificado él la cuenta en cuestión. Sí que consta en el DOCUMENTO 3 que acompaña las alegaciones de fecha 30 de septiembre de 2020, al crearse esta nueva cuenta , se verificó el número del dispositivo móvil asociado a la cuenta ID ***ID.4, el día 27 de mayo de 2019 a las 11:14pm CEST, previo a la realización del pedido fraudulento.

Por último, tampoco ha quedado acreditado que un ciberdelincuente hubiera obtenido los datos de la tarjeta asociada a la dirección de correo electrónico del reclamante en el mercado negro.

No obstante, de no haberse suprimido la cuenta del reclamante, alega el reclamado que habría existido una duplicidad de cuentas y no podría haberse creado una nueva cuenta con idéntica dirección ******EMAIL.1***. Y sí ha quedado establecido que la cuenta desde la que se realizó el pedido fraudulento fue creada el 1 de junio de 2018.

Finalmente, también resulta plausible que el reclamante abriera una nueva cuenta después de la supresión de la anterior (cuarta hipótesis). Alega el reclamado que “esta hipótesis encajaría plenamente con la supresión inicial de los datos y la posterior suplantación de identidad por parte del ciberdelincuente, ya que los datos de la segunda cuenta abierta por el reclamante no habrían sido suprimidos”. En cualquier caso, para haber podido crear esta nueva cuenta debería haberse suprimido

debidamente la creada anteriormente o habría existido duplicidad de cuentas y esto no lo permite el reclamado, según se desprende de las alegaciones por él presentadas.

Por todo lo expuesto, no ha podido acreditarse debidamente en el expediente que la supresión solicitada por el reclamante no hubiera sido atendida correctamente y se hubiesen continuado tratando los datos personales del reclamante careciendo de base jurídica que legitimara tal tratamiento.

Lo anterior ha de conectarse con la vigencia en nuestro Derecho Administrativo sancionador del principio de presunción de inocencia reconocido en el artículo 24.2 de la Constitución Española, de modo que el ejercicio de la potestad sancionadora del Estado, en sus diversas manifestaciones, está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones. El principio de presunción de inocencia impide imputar una infracción administrativa cuando no se haya obtenido y constatado una prueba de cargo que acredite los hechos que motivan la imputación o la intervención en los mismos del presunto infractor.

En el presente caso, no existe ninguna constatación de que la supresión de su cuenta, solicitada por el reclamante, no hubiera sido atendida correctamente y se hubiesen continuado tratando los datos personales del reclamante careciendo de base jurídica que legitimara tal tratamiento, desconociendo la normativa aplicable.

El Tribunal Constitucional (SSTC 131/2003 y 242/2005, por todas) se ha pronunciado en ese sentido al indicar que una de las exigencias inherentes al derecho a la presunción de inocencia es que la sanción esté fundada en actos o medios probatorios de cargo o incriminadores de la conducta imputada y que recae sobre la Administración pública actuante la carga probatoria de la comisión del ilícito administrativo y de la participación en él del denunciado.

Por su parte, el artículo 28.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público establece como uno de los principios de la potestad sancionadora el de la “Responsabilidad” y determina al respecto que:

“*Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa*”.

Igualmente, se debe tener en cuenta lo que establece el artículo 53.2 la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, el cual establece que:

“*Además de los derechos previstos en el apartado anterior, en el caso de procedimientos administrativos de naturaleza sancionadora, los presuntos responsables, tendrán los siguientes derechos: (…)*

> *b) A la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario”.*

Por lo tanto, a tenor de lo anteriormente expuesto, por la Directora de la Agencia Española de Protección de Datos

RESUELVE:

PRIMERO: ARCHIVAR el procedimiento PS/00225/2020, iniciado a la entidad GLOVOAPP23, SL, con CIF: B66362906.

SEGUNDO: NOTIFICAR la presente resolución a la entidad GLOVOAPP23, S.L.

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 LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente 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.

938-131120

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