A LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

D./Dña. [Nombre y Apellidos del Reclamante], mayor de edad, con DNI **[Número de DNI]**, correo electrónico **[correo electrónico]** y domicilio a efectos de notificaciones en **[Dirección completa]**, actuando en nombre y derecho propio, comparece y como mejor proceda en Derecho, **EXPONE:**

Que por medio del presente escrito, y al amparo de lo dispuesto en el Reglamento (UE) 2016/679 (RGPD) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), formula **RECLAMACIÓN** en materia de protección de datos personales contra las siguientes entidades, por los hechos y fundamentos que se detallan a continuación:

ENTIDADES RECLAMADAS

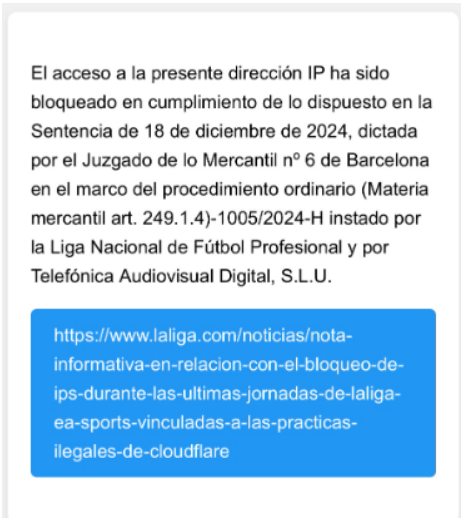
- **TELEFÓNICA DE ESPAÑA, S.A.**, con CIF A82018474 y domicilio social en Calle Gran Vía, 28, 28013, Madrid.
- **VODAFONE ONO, S.A.**, con CIF A62186556 y domicilio social en Avda América, 115, 28042, Madrid.
- **DIGI SPAIN TELECOM, S.L.**, con CIF B84919760 y domicilio social en Calle de Francisca Delgado, 11, 28108, Alcobendas (Madrid).
- **TELEFÓNICA MÓVILES ESPAÑA, S.A.**, con CIF A78923125 y domicilio social en RONDA DE LA COMUNICACION, S/N - DISTRITO C - EDIF. SUR 3, 28050, Madrid.
- **MASORANGE, S.L.**, con CIF B13857198 y domicilio social en PASEO DEL CLUB DEPORTIVO (PQ. EMPRESARIAL LA FINCA), 1 - EDIF. 8, 28223, POZUELO DE ALARCON (Madrid).
- **VODAFONE ESPAÑA, S.A.U.**, con CIF A80907397 y domicilio social en Avda América, 115, 28042, Madrid.

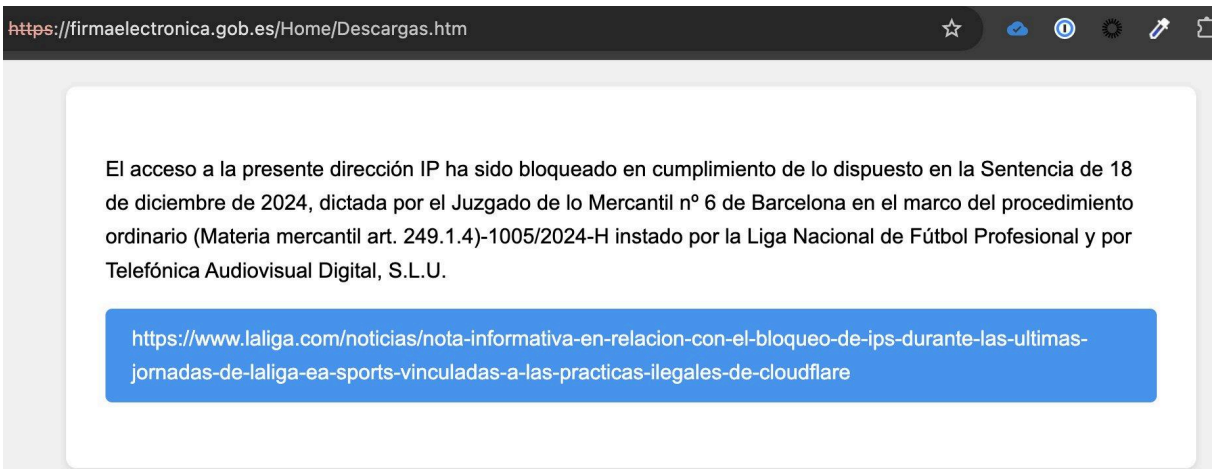
La presente reclamación se fundamenta en los siguientes

HECHOS

PRIMERO.- El reclamante es un usuario de los servicios de comunicaciones electrónicas prestados por las operadoras denunciadas, a través de los cuales accede de forma habitual a contenidos y servicios en Internet.

SEGUNDO.- Las operadoras reclamadas, para ejecutar supuestas órdenes de bloqueo de acceso a determinados recursos online, están implementando una medida técnica que va más allá de un simple bloqueo. Dicha medida consiste en la alteración de los certificados de seguridad (SSL/TLS) de las comunicaciones, lo que en la práctica se conoce como un ataque *"man-in-the-middle"* (hombre en el medio), para mostrar un aviso como el que figura continuación:





Para poder mostrar un mensaje de aviso sobre el bloqueo en el navegador del usuario, la operadora debe, presumiblemente, capturar la petición de conexión y suplantar la identidad del servidor de destino que, de otro modo, estaría protegido por el cifrado de extremo a extremo.

TERCERO.- Esta interceptación activa de las comunicaciones permite a las operadoras acceder al contenido íntegro de las mismas. Esto significa que datos personales de toda índole, tanto del titular del recurso web como de los usuarios que intentan acceder a él (incluyendo datos de navegación, credenciales, contenido de formularios, direcciones de correo electrónico, etc.), son tratados por las operadoras sin que exista consentimiento ni base legitimadora alguna para ello.

CUARTO.- Esta práctica afecta gravemente a los derechos de múltiples actores:

1. **A los titulares de las páginas web afectadas:** Se compromete la seguridad y la confidencialidad de sus comunicaciones y las de sus usuarios, generando una quiebra de confianza y un grave daño reputacional.
2. **A los usuarios de Internet (como el reclamante):** Se vulnera de forma flagrante su derecho fundamental al secreto de las comunicaciones (art.

18.3 de la Constitución Española) y su derecho a la protección de datos personales. El usuario no es informado de que sus comunicaciones están siendo interceptadas y sus datos tratados, y dicha interceptación se produce sin la preceptiva y específica autorización judicial que sería necesaria para levantar el secreto de las comunicaciones.

QUINTO.- La actuación de las operadoras excede manifiestamente cualquier habilitación legal que pudieran ostentar para realizar un simple bloqueo de acceso, constituyendo, cuando menos, un manifiesto abuso de derecho. Una orden judicial de bloqueo no ampara, en ningún caso, la interceptación del contenido de las comunicaciones, que es una medida mucho más intrusiva y que requiere de una ponderación y autorización judicial específica y motivada que aquí no concurre.

FUNDAMENTOS DE DERECHO

I.- Objeto de la reclamación y competencia de la AEPD
La presente reclamación tiene por objeto el presunto tratamiento masivo e ilícito de datos personales llevado a cabo por las operadoras reclamadas, consistente en la interceptación de comunicaciones electrónicas y el acceso a los datos contenidos en las mismas sin una base de legitimación válida.

La competencia de esta Agencia para conocer de los hechos se fundamenta en el Reglamento (UE) 2016/679 (RGPD) y en la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD). En particular, resulta de aplicación lo dispuesto en el artículo 67 de la LOPDGDD, que establece que **"La Agencia Española de Protección de Datos actuará en todo caso cuando sea precisa la investigación de tratamientos que implique un tráfico masivo de datos personales"**, supuesto que concurre en el presente caso dado el número masivo e indeterminado de usuarios afectados por estas prácticas.

II.- Tratamiento ilícito de datos personales por ausencia de base legitimadora (Vulneración del artículo 6 del RGPD)
La interceptación de las comunicaciones de los usuarios para analizar su contenido y mostrar un mensaje de bloqueo encaja plenamente en la definición de "tratamiento" del artículo 4.2 del RGPD. Dicho tratamiento es ilícito al no concurrir ninguna de las bases de legitimación previstas en el **artículo 6.1 del RGPD**. En particular:

- No existe consentimiento del interesado.
- La supuesta "obligación legal" de ejecutar un bloqueo no habilita para realizar un tratamiento de datos tan intrusivo como la interceptación del contenido, que excede lo necesario para cumplir con dicha obligación.

III.- Vulneración de los principios relativos al tratamiento (Vulneración del artículo 5 del RGPD)
La actuación de las reclamadas vulnera, además, los siguientes principios básicos del tratamiento de datos:

- **Principio de minimización de datos (art. 5.1.c):** La interceptación de todo el flujo de comunicación es una medida desproporcionada y no necesaria para cumplir con la obligación de bloqueo, existiendo alternativas técnicas mucho menos intrusivas (como el bloqueo a nivel de DNS) que no implican acceder al contenido de la comunicación.
- **Principio de integridad y confidencialidad (art. 5.1.f):** La interceptación de las comunicaciones, que implica la suplantación de certificados de seguridad, constituye una quiebra flagrante de la seguridad y la confidencialidad de los datos. Esta práctica es, por definición, un tratamiento no autorizado que atenta directamente contra la confidencialidad que los operadores deben garantizar.
- **Principio de licitud, lealtad y transparencia (art. 5.1.a):** El tratamiento se realiza de forma oculta para el usuario, sin que este sea informado en ningún momento de que sus comunicaciones están siendo interceptadas, lo que supone una total falta de transparencia.

IV.- Distinción entre el secreto de las comunicaciones y la protección de datos

Como esta Agencia ha señalado en anteriores resoluciones, el derecho al secreto de las comunicaciones (art. 18.3 CE) y el derecho a la protección de datos (art. 18.4 CE) son derechos fundamentales autónomos. La actuación de las operadoras, al acceder y tratar datos de las comunicaciones sin una base legal válida, constituye una infracción directa de la normativa de protección de datos, competencia de esta Agencia, con independencia de las posibles vulneraciones del secreto de las comunicaciones, que requerirían intervención judicial.

En definitiva, todo apunta a que las operadoras no están simplemente tratando "datos de tráfico", sino interceptando el contenido de las comunicaciones, lo cual es una vulneración flagrante del secreto de las comunicaciones que requiere una autorización judicial específica que no consta en este caso.

Pero incluso si, hipotéticamente, solo accedieran a los "datos de tráfico" para realizar el bloqueo, dicho tratamiento sería ilícito. Sería desproporcionado (vulnerando el Principio de minimización de datos (art. 5.1.c) del RGPD), para una finalidad no prevista (mostrar un mensaje de bloqueo), y sin una base legal válida, contraviniendo la estricta doctrina del TJUE al respecto.

Por todo lo expuesto,

SOLICITO A LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS que, teniendo por presentado este escrito, se sirva admitirlo y, previos los trámites oportunos:

- Acuerde el inicio de un procedimiento de investigación para el esclarecimiento de los hechos denunciados.
- Requiera a las operadoras reclamadas para que informen detalladamente sobre los métodos técnicos que emplean para ejecutar los bloqueos de acceso a recursos web y, específicamente, sobre la forma en que se

muestra el aviso de bloqueo a los usuarios, a fin de determinar si se está produciendo la interceptación de comunicaciones descrita.

- A la vista del resultado de la investigación, y en caso de confirmarse los hechos, acuerde el inicio del correspondiente procedimiento sancionador, imponiendo a las reclamadas las sanciones que en Derecho correspondan por la comisión de las infracciones constatadas.

OTROSÍ DIGO que, para el supuesto de que se inicien actuaciones de investigación o un procedimiento sancionador a resultas de la presente reclamación, solicito que se me reconozca la condición de parte interesada y se me notifiquen todas las actuaciones y resoluciones que se dicten en el curso del mismo.

Por ser todo ello de Justicia que pido en [LUGAR], a [FECHA].
Fdo.: [NOMBRE Y APELLIDOS DEL RECLAMANTE]