



Novedades  
sobre el  
Reglamento  
**ePrivacy**

---

Privacidad  
Marzo 2021

ECIJA

## Análisis de la última versión del Reglamento sobre el respeto a la vida privada y la protección de los datos personales en las comunicaciones electrónicas






La última versión del Reglamento sobre el respeto a la vida privada y la protección de los datos personales en las comunicaciones electrónicas (el Reglamento ePrivacy) ha sido presentada el pasado mes de febrero. Este texto supondrá uno de los pilares fundamentales de la normativa relativa a los derechos digitales y de la protección de la información de los usuarios.

En este sentido, a fecha de redacción de esta nota, en Europa se encuentra vigente la **Directiva 2002/58 de Privacidad y Comunicaciones Electrónicas** (que en España fue transpuesta por **la Ley de Servicios de la Sociedad de la Información 34/2002, la LSSI**). El conocido como **Reglamento ePrivacy**, ha pasado en el mes de febrero, por uno de sus últimos trámites para su aprobación publicándose un nuevo borrador (que debería de ser muy cercano al definitivo) para que sea debatido por el Parlamento Europeo.

En este sentido, el contenido del presente documento pretende detallar las principales novedades y cuestiones que trata esta normativa. No obstante, cabe indicar que el contenido de esta nueva versión del Reglamento ePrivacy podrá sufrir variaciones antes de su definitiva publicación y aplicación.

A modo de introducción, cabe indicar que **el Reglamento ePrivacy incluye, dentro de su ámbito de aplicación el tratamiento de las comunicaciones electrónicas, su contenido o los metadatos que estén referidos a los usuarios finales que se encuentren en la Unión Europea**. De igual manera aplicará a la **protección de la información de los terminales de dichos usuarios, al ofrecimiento de directorios públicos de usuarios finales o al envío de comunicaciones comerciales directas por medios electrónicos a dichos usuarios**.

Estas actividades deberán ser desarrolladas por un **prestador de servicios de la sociedad de la información** (en adelante, el "Prestador") **que se encuentre localizado en la Unión Europea o que tenga acceso a la información indicada en el párrafo anterior sobre ciudadanos de la Unión**<sup>1</sup>. A continuación, resumimos las novedades:

- 1 La norma regula en qué supuestos está autorizado el tratamiento de los datos, del contenido y de los metadatos de las comunicaciones electrónicas y en qué casos será necesario recabar el consentimiento del usuario final. 
- 2 Restricción de la identificación de las llamadas, bloqueo de llamadas entrantes no deseadas, etc. 
- 3 Se prevé la posibilidad de que el consentimiento se obtenga a través del navegador, solicitando al usuario la opción por una configuración determinada en el momento de su instalación, que además sea fácilmente modificable en cualquier momento. 
- 4 Comunicaciones comerciales a clientes: se mantiene el sistema de opt-out (derecho de oposición) siempre que la comunicación se refiera a la comercialización de sus propios productos o servicios contratados. 
- 5 Las sanciones podrán ascender entre los diez millones de euros o un 2% de los beneficios obtenidos por la sociedad o veinte millones o un 4% de los beneficios obtenidos por la sociedad, asemejándose al límite del RGPD. 

<sup>1</sup> El Reglamento ePrivacy no ha sido traducido aún al castellano, por lo que la nomenclatura de algunos términos podrá diferir de la versión final en castellano.



## 1. CONSENTIMIENTO

---

Respecto al consentimiento, el Reglamento ePrivacy hace suyas como **válidas las disposiciones recogidas en el RGPD para la otorgación del mismo, tanto para personas físicas como jurídicas**. Este último punto, no quedaba definido como tal en el RGPD.

Asimismo, una de las novedades introducidas es que **da prevalencia al consentimiento directamente expresado por un usuario sobre aquel otro prestado utilizando los ajustes de los programas informáticos que permitan dichas comunicaciones electrónicas**. Este último punto es fundamental, **puesto que permite recabar el consentimiento del usuario final a través de la configuración, por ejemplo, del navegador**.

A su vez, en aquellos casos en los que un prestador no pueda identificar al interesado, para demostrar que ha otorgado el consentimiento, **será suficiente el protocolo técnico que demuestre que se prestó el consentimiento desde un equipo conectado a la interfaz de una red pública de telecomunicaciones para transmitir, tratar o recibir información**.

Finalmente, **a aquellos usuarios que consientan el tratamiento de datos de comunicaciones electrónicas, se les tendrá que recordar periódicamente (mínimo cada 12 meses y siempre que el tratamiento persista), la posibilidad de retirar el consentimiento prestado**. Esta obligación desaparecerá solo si ha solicitado no recibir dichos recordatorios.

En relación **con el tratamiento de datos de comunicaciones electrónicas, solo se permitirá cuando sea necesario para prestar el servicio de comunicaciones electrónicas, para detectar o prevenir riesgos para la seguridad o ciberataques o por ser necesario para el cumplimiento de una obligación legal**.

Salvo para el último supuesto previsto, **el tratamiento solo se permitirá durante el plazo necesario para la finalidad establecida, o en caso de no poder cumplirse, anonimizando los datos**.

Respecto del contenido de las comunicaciones electrónicas, los prestadores solo podrán tratar, entre otros, texto, voz, vídeo, imágenes y sonidos, sin perjuicio de lo anteriormente establecido:

- Cuando, **con el consentimiento del usuario y para su uso individual, se requiera prestar un servicio solicitado**; o
- **Si todos los usuarios finales afectados han dado su consentimiento al tratamiento de sus contenidos para uno o varios fines específicos**. En este caso, **será necesario realizar con anterioridad, una PIA para analizar el impacto en el tratamiento previsto e incluso, consultar a la autoridad de control correspondiente**.

De la misma manera a lo ya mencionado, destacamos los escenarios en los que se permitirá **el tratamiento de metadatos en comunicaciones electrónicas y, por tanto, de datos que permitirán rastrear e identificar el origen y el destino de una comunicación, la ubicación del dispositivo, así como la fecha, la hora, la duración y el tipo de comunicación**:

- Por ser **necesario a efectos de gestión u optimización de la red o para cumplir los requisitos técnicos de calidad del servicio**.
- Para la **ejecución de un contrato de servicios de comunicaciones electrónicas, o en caso de ser necesario para la facturación, el cálculo de los pagos de interconexión, la detección o el cese del uso fraudulento o abusivo de los servicios de comunicaciones electrónicas o la suscripción a los mismos**;



- En caso de haber prestado **consentimiento** para tal fin.
- Por ser necesario para la **protección de intereses vitales**;
- Respecto a los **metadatos de localización necesarios para fines de investigación científica, histórica o con fines estadísticos**, cumpliendo una serie de requisitos.
- Con relación al resto de metadatos también necesarios para las finalidades indicadas en el punto anterior, se **requerirá garantías adecuadas conforme a lo previsto en el artículo 21.6) y 89.1), 2) y 4) del RGPD**.



Respecto a los **tratamientos de metadatos considerados compatibles en comunicaciones electrónicas**, cuando el tratamiento sea para un fin distinto a aquel para el que fueron recogidos inicialmente, y no se base en el consentimiento del usuario ni en una norma de un Estado miembro o de la Unión, se requiere que el prestador **compruebe si el tratamiento de los metadatos para este nuevo fin es compatible con el inicialmente dispuesto**, teniendo en cuenta para ello aspectos como la relación entre la finalidad inicial y la prevista posteriormente para el nuevo tratamiento, el contexto en el que se recogieron los metadatos, la relación entre el usuario y el proveedor, la naturaleza del metadato, las consecuencias que para el usuario podría acarrear el nuevo tratamiento y si existen garantías adecuadas, como el cifrado y la seudonimización de los datos.

En caso de considerar este tratamiento compatible, solo podrá llevarse a cabo teniendo en cuenta:

- **Que el tratamiento no pueda realizarse con información anonimizada**, y que los metadatos sean eliminados o anonimicen en cuanto dejen de ser necesarios para la finalidad prevista;
- **Que el tratamiento se limite a los metadatos que se han seudonimizados**, y
- **Que los metadatos no se utilicen para determinar la naturaleza, características o para elaborar un perfil de un usuario**.

Por último, y tal y como hemos venido indicando, el Reglamento ePrivacy obliga a los prestadores a **eliminar o anonimizar los datos cuando dejen de ser necesarios para las finalidades previstas o, en determinados casos**, cuando dejen de ser necesarios para prestar un servicio de comunicaciones electrónicas.

## 2. COOKIES Y TECNOLOGÍAS SIMILARES

---

Otra de las novedades introducidas en el Reglamento ePrivacy son las novedades relativas a las cookies y tecnologías similares.





En este sentido, **se mantiene la prohibición del tratamiento de dicha información con las siguientes excepciones:**

- Que dicho **tratamiento sea necesario para prestar el servicio de comunicaciones electrónicas.**
- Que **el usuario lo haya consentido.**
- Que **sea estrictamente necesario para prestar un servicio específicamente requerido por el usuario final.**
- **Que sea necesario para la finalidad de medición de audiencias.**
- Que sea **necesario para finalidades de seguridad, prevención del fraude o detectar fallos técnicos.**
- Que sea **necesario para una actualización de software**, siempre que sea necesario, el usuario sea informado y el usuario final pueda apagar la instalación automática de dichas actualizaciones.
- Que sea **necesario para localizar el terminal del usuario final en una llamada de emergencia.**

**En el caso de que la información recogida se fuera a utilizar con una finalidad diferente, el prestador deberá analizar la compatibilidad de dichas finalidades teniendo en cuenta la relación entre el tratamiento inicial y subsiguiente, el contexto y la relación entre el usuario final y el prestador, la naturaleza y las modalidades del tratamiento posterior y la existencia de medidas adicionales, como cifrado y seudonimización.**

Como se ha analizado en el punto anterior, el tratamiento **únicamente será acorde si la información es borrada o anonimizada cuando no fuera necesaria, el tratamiento fuera referido a información seudonimizada y la información no es utilizada para determinar la naturaleza o características del usuario final o para construir un perfil del mismo.**

### **3. CONTROL SOBRE COMUNICACIONES ELECTRÓNICAS Y LLAMADAS COMERCIALES**

---

El Capítulo III regula los derechos de los usuarios finales en relación con el control sobre las comunicaciones electrónicas. Los arts. 12 y 13 del Reglamento ePrivacy **establecen reglas aplicables a la identificación de los abonados.** A modo de ejemplo, **el derecho a impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea del usuario en las llamadas salientes (recogido en la letra m) del art. 47.1) ahora deberá poder ejercerse por llamada, por conexión o de forma permanente.** Asimismo, se **introduce un nuevo derecho centrado en la posibilidad de impedir, por parte del usuario llamado, la presentación de la identificación de la línea a la que el llamante está conectado.** Todos estos derechos deberán incluir llamadas realizadas a o con origen en los Estados miembros, por lo que tienen un alcance intracomunitario.

Las **excepciones a los derechos mencionados se aplican, por una parte, a casos de llamadas por parte de los servicios de llamadas de urgencia o las realizadas a servicios de urgencia, como el 112.** Por otra parte, se añade una **excepción específica para los casos en los que el usuario final haya impedido el acceso al Sistema Global de Navegación por Satélite (GNSS por sus siglas en inglés) de su equipo terminal: en caso de que se realice una llamada de emergencia, este servicio podrá acceder a la geolocalización del equipo terminal desde el que llama el usuario para la "finalidad de dar respuesta a este tipo de llamadas".**

En relación a las llamadas no solicitadas, el art. 14 del Reglamento ePrivacy deja **en manos de los Estados miembros el desarrollo de pautas específicas destinadas a regular las obligaciones de los operadores en materia de identificar, de forma temporal, a los**



**llamantes en caso de que el usuario llamado solicite el seguimiento de llamadas no solicitadas o maliciosas.** Igualmente, el Reglamento recuerda **que los operadores deberán ofrecer a los abonados, de forma gratuita, la posibilidad de bloquear llamadas entrantes de número específicos, anónimos o con un prefijo o código determinado,** donde sea técnicamente posible, y de detener el reenvío automático de llamadas por un tercero al equipo terminal del usuario.

Como regla general, **la inclusión en los directorios públicos o guías únicamente podrá hacerse con el consentimiento del abonado.** Sin embargo, se da un margen a los Estados miembros para la inclusión de los números de abonados en las guías sin su consentimiento, siempre y cuando el abonado pueda oponerse a dicha inclusión. El art. 15.4a aclara que, **para todos los números incluidos en las guías con anterioridad a la entrada en vigor del Reglamento ePrivacy, dichos números pueden conservarse salvo que el abonado haya expresado su oposición.**

Por último, el art. 16 se ocupa de establecer **reglas concernientes al envío de comunicaciones comerciales y no solicitadas.** Como regla general, **únicamente podrán realizarse los envíos si se cuenta con el consentimiento del destinatario.** Sin embargo, como excepción, **se sigue contemplando el interés legítimo para evitar recoger el consentimiento del destinatario, siempre y cuando a dicho destinatario se le haya ofrecido la oportunidad de oponerse al envío de comunicaciones comerciales tanto en el momento de recogida de sus datos para esta finalidad, como en cada una de las comunicaciones.**

Adicionalmente, **cada comunicación deberá identificar al remitente y utilizar una dirección de respuesta efectiva, lo que podría suponer que ya no sería válido enviar comunicaciones comerciales desde las direcciones que comiencen por “noreply”.** Por último, el Reglamento ePrivacy **aclara que los Estados miembros podrán establecer los períodos de tiempo desde la compra de un producto o servicio durante los cuales un usuario se consideraría cliente.**

Con respecto a las sanciones, se determina que cada usuario final tendrá el derecho a realizar una reclamación sobre las infracciones del Reglamento ePrivacy y **podrá recibir una compensación económica por dichos incumplimientos.**

La graduación de las **sanciones podrá ascender entre los diez millones de euros o un 2% de los beneficios obtenidos por la sociedad o veinte millones o un 4% de los beneficios obtenidos por la sociedad, asemejándose al límite del RGPD.**

Para terminar, **el Reglamento ePrivacy, cuando sea finalmente publicado, tendrá un plazo de 24 meses para su plena aplicación derogando la anterior Directiva 2002/58.**

---

**Área de Protección de Datos y Privacidad**

+ 34 91 781 61 60

info@ecija.com





# ECIJA

Torre de Cristal  
Pº de la Castellana, 259C  
28046 Madrid

---

[www.ecija.com](http://www.ecija.com)