CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

RESOLUCIÓN N°	23	2026

Montevideo, 11 de setiembre de 2026

VISTO: la necesidad de ampliar lo resuelto por este Consejo Ejecutivo con relación a las soluciones técnicas para evitar la indexación de contenidos publicados en internet, que puedan afectar el derecho a la Protección de Datos Personales en sitios web de organismos públicos.

RESULTANDO: 1. Que esta Unidad se pronunció a través de la Resolución N° 1040/012, de 20 de diciembre de 2012, sobre las posibles soluciones técnicas para evitar que ciertos contenidos publicados en sitios web que incluyeran información personal fueran indexados e incluidos en el caché de motores de búsqueda;

2. que la mencionada resolución fue dictada en consideración a la situación vigente en ese momento, teniendo presente no sólo la necesidad de brindar soluciones a las personas que procuraban ejercer sus derechos de rectificación, actualización o supresión, sino también la responsabilidad de los organismos públicos editores de sitios web, en su calidad de responsables de tratamiento, todo en el marco de lo establecido en la Ley N° 18.331, de 11 de agosto de 2008;

3. que, posteriormente y en particular en el dictamen N° 14/019, de 30 de setiembre de 2019, la Unidad se pronunció sobre la responsabilidad específica de las empresas titulares de motores de búsqueda a quienes se les atribuyó también el rol de responsables de tratamiento de conformidad con la Ley N° 18.331, y de otros editores de sitios web fuera del ámbito público, haciendo aplicables las recomendaciones de la mencionada resolución;

4. que las medidas sugeridas en la referida resolución N° 1040/012 se sustentaron en informe técnico del Centro Nacional de Repuesta a Incidentes de Seguridad

Informática (CERTuy) de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC), resumiéndose en: a) que los documentos se generen en tiempo real en lugar de que sean generados previamente, de forma que no se puedan almacenar por no existir al momento en que se buscan, controlando su propagación; b) que la publicación de información con datos personales se efectúe en formato imagen con etiquetas o atributos que no contengan esos datos;

5. que la operativa actual de las búsquedas en internet ha cambiado, orientándose hacia el uso de chatbots -sistemas conversacionales provistos por distintas empresas u organizaciones que comprenden instrucciones de las personas y generan respuestas interactuando con éstas mediante lenguaje natural-, asistentes virtuales –que incorporan a las funciones anteriores la posibilidad de interactuar con otros servicios-, y agentes de Inteligencia Artificial –que poseen un mayor grado de autonomía y ejecutan acciones para alcanzar objetivos predefinidos-. A efectos de contextualizar las instrucciones brindadas y elaborar sus respuestas, estos sistemas emplean distintos mecanismos de búsqueda y recopilación de información –incluyendo datos personales- en internet y otras fuentes; mecanismos que incluyen el rastreo web y la indexación de contenido, la consulta en tiempo real (mediante APIs y otros) y el acceso a fuentes privadas.

CONSIDERANDO: 1. Que la publicación de datos personales en internet se constituye en una hipótesis de aplicación del artículo 17 de la Ley N° 18.331, de 11 de agosto de 2008, que regula el derecho a la comunicación de datos personales, y dispone que éstos sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos –o alguna de sus excepciones-;

2. que, a su vez, el artículo 9° Bis de la ley citada prevé un listado taxativo de fuentes públicas de información habilitantes del tratamiento de datos personales, por lo que resulta imprescindible analizar la fuente del dato personal para determinar la licitud del tratamiento de ese dato, en tanto internet en sí misma no se encuentra incluida dentro de ese listado;

3. que más allá de la responsabilidad asociada al tratamiento de los datos por parte de las empresas proveedoras de chatbots, asistentes virtuales y agentes de Inteligencia Artificial, existe una responsabilidad de quienes publican la información en los sitios web, cuando en esta información se encuentran contenidos datos personales;

4. que el alcance de la responsabilidad de los responsables de tratamiento fue objeto de modificaciones a través del artículo 39 de la Ley N° 19.670, de 15 de octubre de 2018, modificando el artículo 12 de la Ley N° 18.331, a fin de incorporar el concepto de responsabilidad proactiva, reglamentado posteriormente en los artículos 5° y siguientes del decreto N° 64/020, de 17 de febrero de 2020;

5. que, en lo que refiere específicamente a la provisión de soluciones técnicas para evitar la indexación de contenidos publicados en internet que puedan afectar el derecho a la protección de datos personales, corresponde ampliar el alcance subjetivo de la Resolución N° 1040/012 de este Consejo Ejecutivo con carácter general, incluyendo a todo responsable o encargado que publique este tipo de contenidos en sitios web, y no sólo a organismos públicos;

6. que, adicionalmente, corresponde aclarar que las soluciones técnicas a adoptar no sólo responden a los mecanismos empleados por motores de búsqueda sino también a aquellos empleados por chatbots, asistentes virtuales y agentes de Inteligencia Artificial o sistemas similares;

7. que, dentro de esas soluciones se encuentran las indicadas en la precitada Resolución N° 1040/012, y otras tales como las restricciones de acceso a los sitios web mediante mecanismos de autenticación o similares, la configuración de robots.txt, el etiquetado para evitar la indexación, el uso de WAFs, u otros, que deberán ser evaluados por el responsable o encargado, con el asesoramiento de su delegado de protección de datos personales, en caso de haber sido designado.

ATENTO a lo expuesto,

El Consejo Ejecutivo de la Unidad de la Unidad Reguladora y de Control de Datos Personales

RESUELVE:

1. Indicar a los responsables y encargados de tratamiento del ámbito público y privado, que a efectos de cumplir con el principio de responsabilidad proactiva previsto en el artículo 12 de la Ley N° 18.331, de 11 de agosto de 2008 –en la redacción dada por el artículo 39 de la Ley N° 19.670, de 15 de octubre de 2018- deberán considerar la aplicación de mecanismos para evitar la recopilación, indexación y posterior tratamiento de datos personales que publican en sus sitios web, por motores de búsqueda, chatbots, asistentes virtuales y agentes de Inteligencia Artificial, y sistemas similares.
2. Los mecanismos a aplicarse en el caso concreto deberán considerar lo previsto en la presente Resolución, en el documento que se anexa al presente y forma parte integrante de la misma, y en especial, lo recomendado por el delegado de protección de datos personales, en caso de haber sido designado.
3. En los casos de entidades públicas, la determinación de los mecanismos antedichos resulta de especial trascendencia, de forma de compatibilizar el derecho a la protección de datos personales con las obligaciones de transparencia activa en formato de dato abierto y de accesibilidad previstas en el artículo 5° de la Ley N° 18.381, de 17 de octubre de 2008, el artículo 82 de la Ley N° 19.355, de 19 de diciembre de 2015, el artículo 88 de la Ley N° 19.924, de 18 de diciembre de 2020 y sus respectivas reglamentaciones.
4. Se recomienda en especial que se incorporen en los términos y condiciones del sitio, cláusulas contractuales que informen a empresas titulares de motores de búsqueda, chatbots, asistentes virtuales y agentes de Inteligencia Artificial, entre otras, las eventuales restricciones de uso de la información publicada cuando existan datos personales.
5. En todos los casos, y a efectos de garantizar el derecho a la información previsto en el artículo 13° de la Ley N° 18.331, se recomienda incluir en las políticas de privacidad del sitio y mantener en todos los casos disponible, el alcance de las medidas adoptadas para evitar la recopilación, indexación y posterior tratamiento de los datos personales de los titulares de los datos.
6. Indicar a los titulares de los datos que el ejercicio de los derechos referidos en los artículos 13° y siguientes de la Ley N° 18.331, de conformidad con lo previsto en el dictamen N° 14/019, de 30 de setiembre de 2019, podrá realizarse no sólo

con respecto a los titulares de los sitios web, sino también con respecto a las empresas proveedoras de motores de búsqueda, chatbots, asistentes virtuales y agentes de Inteligencia Artificial.

7. Como corolario de lo anterior, en todos los casos deberá tenerse presente, de corresponder, lo previsto en el artículo 37 de la Ley N° 19.670, de 15 de octubre de 2018, así como el alcance de las posibilidades efectivas de actualización, rectificación y supresión de información contenida en las fuentes empleadas por estos sistemas, sugiriéndose consultar los términos y condiciones y políticas de privacidad correspondientes, y prever el eventual ejercicio directo de dichos derechos ante el editor del sitio web.
8. PUBLÍQUESE.



ANEXO

Ejemplos de aplicación de mecanismos de desindexación de contenidos que contengan datos personales en sitios web

1. **Mecanismos de autenticación**

Se trata de sistemas tales como usuario y contraseña, acceso mediante certificados o tokens de acceso, o autenticaciones multifactor, que en los hechos impiden técnicamente el acceso a aquellos que no acrediten su identidad o una autorización particular, efectuando en definitiva un efectivo control de acceso a un determinado sitio web, o parte de éste, según el nivel de granularidad configurado.

En estos casos, no podrá leerse en contenido del sitio, por lo que no podrá emplearse para responder las preguntas o incorporarlo en los procesos de los chatbots, asistentes virtuales y agentes de Inteligencia Artificial, o similares.

2. **Robots.txt**

Refiere a archivos de texto ubicados en la raíz de un sitio y que genera una indicación a los robots automatizados empleados por distintas empresas y organizaciones qué partes del sitio no pueden rastrear. Es posible establecer esta condición sólo a determinado robot o a todos los robots, siendo esta la alternativa preferida para limitar todo tipo de rastreo:

User-agent: *

Disallow: /carpetaprivada/

Allow: /

En el ejemplo, se establece una regla general para todos los robots, evitando el rastreo al contenido de la carpeta denominada “carpetaprivada”, y habilitándolo para el resto del sitio.

Si se pretende evitar el rastreo de todo el sitio, la regla sería:

User-agent: *

Disallow: /

Ahora bien, si lo que se pretende es evitar el rastreo únicamente de un contenido en especial, la regla sería:

User-agent: *

Disallow: /resolucionesydictamenes/resolucion14-033.pdf

En este último caso, la restricción es para todo tipo de robot, únicamente con respecto a la resolución mencionada, que se encuentra ubicada en la carpeta de resoluciones y dictámenes.

3. Etiquetado

En el caso del etiquetado, es posible emplear etiquetas en el encabezado de una página, solicitando a los robots que no indexen la página y no sigan los enlaces que ésta contiene. Sin perjuicio de la posibilidad de dar directivas específicas, se estima convenientes una indicación genérica que puede traducirse en:

<meta name= “robots” content= “noindex, nofollow”>

Existen otros tipos de etiquetados, como el encabezado HTTP, que implica la colocación de una etiqueta en la cabecera HTTP, del estilo:

</> http

X-Robots-Tag: noindex

Este mecanismo puede resultar de utilidad para caso de archivos de imágenes, videos y recursos que no contienen HTML.

4. WAF (Web Application Firewall)

Se trata de un sistema de seguridad que se coloca entre internet y un sitio web y permite inspeccionar, controlar y filtrar solicitudes HTTP o HTTPS antes de que lleguen al servidor. Si bien se emplean fundamentalmente para protección ante ataques, pueden también ser útiles para controlar el acceso de bots usados, por ejemplo, por motores de búsqueda o sistema de IA en general. En los hechos, este sistema impide el acceso efectivo al sitio web.

Los ejemplos brindados arriba no procuran agotar la casuística de medidas pasibles de ser adaptadas por responsables y encargados con los objetivos mencionados en la Resolución de la que forma parte este Anexo, y son parte de la valoración que deben realizar responsables y encargados –junto con sus delegados de protección de datos en caso de haber sido designados- para cumplir con el principio de responsabilidad proactiva y el principio de seguridad de los datos previstos en la legislación vigente.