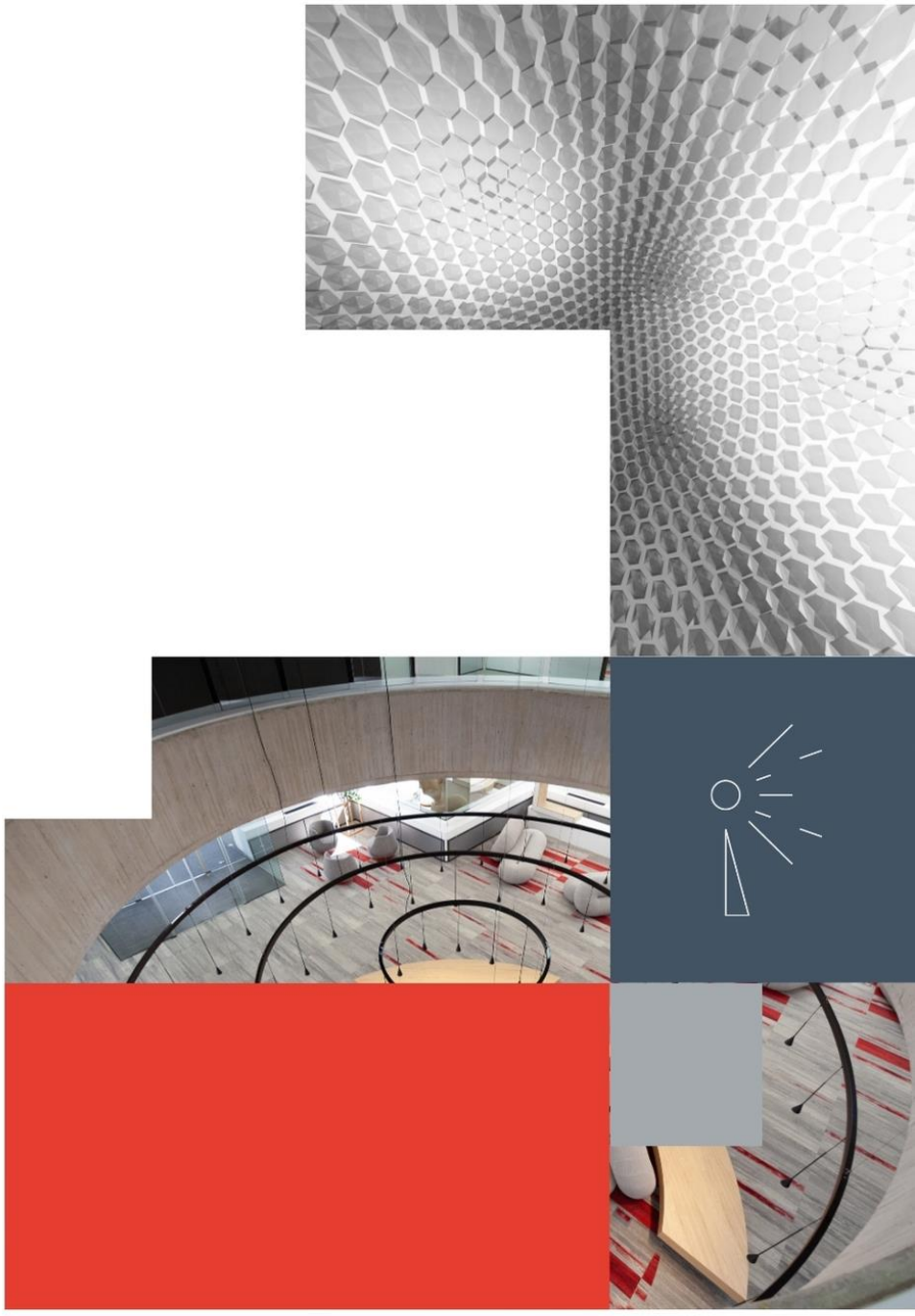
ECIJA

14.02.2024

Privacidad en la DSA

Nota informativa



Privacidad en la DSA

Sin perjuicio de que Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE ("**DSA**" por sus siglas en inglés) tiene su enfoque principal en la regulación de las plataformas en línea, los servicios de intermediación y las redes sociales para abordar la difusión de contenido ilegal y proteger la seguridad de los usuarios en línea, la privacidad y la protección de datos personales también son objeto de especial regulación, así como de advertencias, toda vez que forman parte intrínseca de los servicios digitales.

En este sentido, aunque la DSA y el Reglamento (UE) 2016/679 de Protección de Datos Personales ("RGPD") no compartan la misma taxonomía de sujetos pasivos, el amplio alcance de las definiciones de la RGPD en cuanto a los "responsables del tratamiento" y el "tratamiento de datos personales" implica que todos los intermediarios sujetos a la DSA también son susceptibles de ser considerados responsables del tratamiento bajo la RGPD en relación con cualquier procesamiento de datos personales en el que participen y para el cual establezcan medios de tratamiento.

Así, los prestadores de plataformas en línea también podrían ser considerados como "encargados del tratamiento" bajo la RGPD, y esta superposición activaría la aplicación de ambas regulaciones. Sin embargo, de acuerdo con lo señalado en el artículo 2 apartado 4 letra g) de la DSA, el reglamento nunca debe ser aplicado en perjuicio de lo señalado en el RGPD, pues en lo que a protección de datos se refiere, este último tendría prevalencia por su carácter de *lex specialis*.

La excepción a lo anterior aplica en cuanto a las reglas de responsabilidad de los intermediarios en la DSA, las cuales tendrían prevalencia sobre la RGPD, pues esta última se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE de Comercio Electrónico en el Mercado Interior (artículo 2 apartado 4 de la RGPD).

De esta forma, hacemos notar que la DSA menciona a la RGPD 19 veces a lo largo de sus considerandos y artículos, asignando un rol importante al concepto de "elaboración de perfiles", tal y como es definido en la RGPD, en las obligaciones fundamentales para todas las plataformas en línea.

Esto crea una telaraña compleja de disposiciones legales donde destaca la interacción entre estos dos marcos legales, y de cara la aplicabilidad de la DSA el próximo 17 de febrero de 2024, hacemos un breve listado en donde resalta esta relación:

1. Prohibición de los Dark Patterns

Los *Dark Patterns*, definidos en el Considerando 67 de la DSA, son prácticas que afectan negativamente la capacidad de los usuarios para tomar decisiones libres e informadas, ya sea intencionalmente o en la práctica. Tanto la RGPD como la DSA se dirigen a estas acciones, directa o indirectamente. En el caso de la RGPD, sus disposiciones protegen contra el diseño manipulativo en el procesamiento de datos personales, resaltando la importancia de la minimización de datos, el consentimiento informado y la Protección de Datos desde el Diseño y por Defecto.

Por su parte, el Artículo 25 de la DSA prohíbe que las plataformas en línea diseñen sus interfaces de manera que engañen o manipulen a los usuarios, limitando su capacidad de decidir libremente. Esta restricción se aplica específicamente a las plataformas en línea definidas en el Artículo 3(i) de la DSA y excluye las prácticas ya cubiertas por la Directiva de Prácticas Comerciales Desleales o el RGPD. Además, el Artículo 25(3) indica que la Comisión emitirá directrices sobre la aplicación de esta prohibición, buscando claridad y coherencia en su implementación, en colaboración con las Autoridades de Protección de Datos.

La prohibición parece aplicable solo a las plataformas en línea tal como y como son definidas en el artículo 3(i)de la DSA, sobre todo considerando que la DSA especifica que la prohibición de *Dark Patterns* no aplica a aquellas prácticas cubiertas por la Directiva de Prácticas Comerciales Desleales o la RGPD.

En este sentido, el mismo artículo 25, apartado 3 de la DSA destaca que la Comisión está facultada para emitir directrices sobre cómo la prohibición de los Dark Patterns será aplicada a prácticas específicas, por lo que se espera mayor claridad. Y dado que la protección otorgada por la RGPD contra los diseños manipulativos seguirá siendo de relevancia, y, sobre todo, de aplicabilidad, será esencial para su consistencia que estas directrices sean desarrolladas en estrecha colaboración con las autoridades de protección de datos.

2. Protección de los menores

Considerando que la protección de los menores es un importante objetivo político para la Unión Europea, la DSA establece en su artículo 28 la obligación de establecer medidas adecuadas y proporcionadas para garantizar un elevado nivel de privacidad, seguridad y protección de estos en su servicio.

En este sentido, los prestadores de plataformas en línea no deben presentar anuncios basados en la elaboración de perfiles mediante la utilización de datos personales del destinatario del servicio cuando "sean conscientes con una seguridad razonable de que el destinatario del servicio es un menor". No obstante, es importante considerar que esta prohibición no debe ser incentivo para los prestadores en línea de mantener, obtener o tratar más datos personales de los que ya dispone para determinar si el destinatario de su servicio es un menor. Esto es por la obligación impuesta por el artículo 5, apartado 1, letra c) de la RGPD, en la cual se establece el principio de minimización de los datos.

No obstante, tal y como es destacado en un informe reciente del *Future Privacy Forum*[1] sobre tecnologías de verificación de edad, estas pueden requerir necesariamente el procesamiento de datos personales adicionales de los requeridos normalmente por el funcionamiento de la plataforma en línea.

3. Prohibición de elaboración de perfiles para mostrar anuncios basados en datos sensibles

El artículo 26, apartado 3 de la DSA obliga a los prestadores de plataformas en línea a no presentar a los destinatarios del servicio anuncios basados en la elaboración de perfiles que utilicen las siguientes categorías especiales de datos personales, que se encuentran listadas en el art. 4.4. de la RGPD: datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

4. Transparencia y responsabilidad en el uso de algoritmos

El artículo 26, apartado 1, letra d) de la DSA impone a la grandes plataformas en línea (VLOP) y a los motores de búsqueda de gran tamaño (VLOSE), la obligación de publicar información sobre aquellos parámetros que son utilizados para determinar la publicidad que es dirigida a los usuarios, lo cual implica el tratamiento de datos personales. Adicionalmente, los prestadores de plataformas en línea deberán publicar en la misma sección las vías a la disposición del usuario para poder modificar dichos parámetros a unos que se ajusten más a su preferencia.

Particularmente, esta obligación busca proporcionar a los usuarios con información clara sobre aquello que ven, incluyendo el origen del contendido al que son expuestos y la base de su personalización. El objetivo es aumentar la transparencia y permitir que los usuarios comprendan la razón por la cual cierto contenido es puesto a la vista, promoviendo así una mayor conciencia sobre el uso de sus datos personales.

5. Eliminación de contenido ilegal, vinculado con el derecho de supresión o rectificación y establecimiento de mecanismos para ello

La DSA establece, de acuerdo con su artículo 16, que los prestadores de plataformas en línea deben eliminar todo contenido ilegal basándose en un mecanismo de aviso y acción, tras la notificación de cualquier individuo o entidad. En paralelo, el artículo 17 de la RGPD permite a los individuos solicitar la eliminación de sus datos personales bajo ciertas condiciones, reforzando así el control sobre el uso de su información personal. Siguiendo el mismo orden de ideas, el artículo 3(h) de la DSA define "contenido ilegal" de una manera amplia, por lo cual, en la medida en que "contenido ilegal" se encuentre relacionado con datos personales (datos personales tratados de forma no legal) ambas normativas se podrían complementar en la forma de abordar la gestión de contenido ilegal y la protección de datos personales, pues permitiría a los individuos elegir la vía legal más adecuada para solicitar la eliminación de dicho contenido.

[1] https://fpf.org/blog/new-fpf-infographic-analyzes-age-assurance-technology-privacy-tradeoffs/

A modo de ejemplo, en lo que respecta a la eliminación de contenido ilegal, la DSA no determina un plazo específico, sino que simplemente requiere actuar "sin demoras indebidas". Por otro lado, el RGPD especifica un marco temporal más definido para atender solicitudes de eliminación de datos, estableciendo un plazo máximo de un mes (ampliable en casos de especial complejidad). Así, los servicios de alojamiento y plataformas en línea sujetos al RGPD pueden utilizar sus procedimientos internos previamente establecidos para gestionar las solicitudes de eliminación de contenido ilegal para atender aquellas obligaciones impuestas por la DSA.

6. Evaluación de riesgos derivados del funcionamiento del servicio en relación con la correspondiente EIPD

La DSA impone a los VLOPs/VLOSEs la obligación de llevar a cabo evaluaciones de riesgo anuales para identificar, analizar y evaluar los riesgos sistémicos originados por el diseño y funcionamiento de sus servicios, incluyendo los sistemas algorítmicos, según establece el Artículo 34. Paralelamente, es probable que estas entidades deban realizar Evaluaciones de Impacto sobre la Protección de Datos (EIPD) conforme al Artículo 35 del RGPD, especialmente cuando sus operaciones de procesamiento, como la utilización de datos personales en sistemas de recomendación o la creación de perfiles de usuarios, activan esta necesidad. Las EIPD son esenciales cuando el procesamiento de datos personales, especialmente con tecnologías emergentes, presenta un alto riesgo para los derechos y libertades individuales.

La DSA especifica cuatro riesgos sistémicos a considerar: la difusión de contenido ilegal; impactos negativos, reales o potenciales, sobre derechos fundamentales específicos, incluyendo la privacidad y la protección de datos; efectos adversos en el discurso cívico, los procesos electorales y la seguridad pública; y repercusiones negativas en temas de violencia de género, salud pública, protección de menores, y el bienestar físico y mental. Las EIPD, por su parte, deben evaluar cómo el procesamiento de datos personales por nuevas tecnologías puede afectar a los derechos y libertades, incluyendo medidas para mitigar estos riesgos. Al realizar estas evaluaciones, los VLOPs/VLOSEs deben considerar cómo factores detallados en el Artículo 34(2) inciden en los riesgos identificados, los cuales se encuentran relacionados en su mayor parte con el procesamiento de datos personales.

Ambas evaluaciones, tanto de la DSA como del RGPD, son medidas preventivas que requieren interacción, en determinados casos, con autoridades regulatorias, y aunque tienen objetivos distintos —la DSA se enfoca en riesgos sistémicos más amplios y la EIPD en riesgos específicos para la protección de datos—, presentan áreas de intersección significativas cuando se trata del procesamiento de datos personales. Consideramos crucial que las EIPD informen y complementen las evaluaciones de riesgo de la DSA, asegurando una implementación coherente y alineada con los marcos regulatorios.

Conclusiones

La interrelación entre la DSA y el RGPD crea un escenario complejo de superposiciones legislativas que exige una aplicación y cumplimiento coherente y eficiente de ambas normativas. Aunque esta dinámica presenta el desafío de posibles inconsistencias, es imperativo abordarlas mediante una interpretación y aplicación uniformes de las leyes. Sin embargo, la estructura actual de aplicación y supervisión de la DSA no establece formalmente un mecanismo de cooperación o coordinación entre el coordinador de servicios digitales y las Autoridades de Protección de Datos, el Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos (que por especialidad de la materia y el ámbito competencial atribuido entenderán de las cuestiones relacionadas con la protección de los datos personales de los usuarios. Sin embargo, esta ausencia no debe ser interpretada como un obstáculo, sino como una oportunidad para desarrollar procesos internos de colaboración. La implementación de la DSA no solo pondrá de manifiesto la complejidad inherente a la interacción entre estos dos importantes marcos legislativos, sino que también subrayará la necesidad de una cooperación efectiva para garantizar un enfoque armonizado en la protección de datos y los servicios digitales a lo largo de la Unión Europea.

Área de TMT
ECIJA
info@ecija.com
Telf: + 34 91.781.61.60

Calle Serrano, 69.
28006 Madrid
www.ecija.com