COMISIÓN
EUROPEA

Bruselas, 26.5.2021
COM(2021) 262 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES

Orientaciones de la Comisión Europea sobre el refuerzo del Código de Buenas Prácticas en materia de Desinformación

1 INTRODUCCIÓN

La crisis de la COVID-19 ha ilustrado claramente las amenazas y desafíos que la desinformación supone para nuestras sociedades. La «infodemia» (la rápida propagación de información falsa, imprecisa o engañosa sobre la pandemia) ha supuesto riesgos sustanciales para la salud de las personas, los sistemas de salud pública, la gestión eficaz de la crisis, la economía y la cohesión social. La pandemia también ha elevado la función que desempeña la tecnología digital en nuestras vidas, haciendo que esta tenga un papel cada vez más central en la forma en que trabajamos, aprendemos, socializamos, satisfacemos las necesidades materiales y participamos en el discurso cívico. Ha planteado grandes retos a la hora de garantizar que el ecosistema digital sea un espacio seguro, y ha mostrado que, a pesar de los importantes esfuerzos realizados hasta la fecha, existe la necesidad urgente de intensificar dichos esfuerzos para luchar contra la desinformación[1].

Desde su origen[2], la línea de actuación contra la desinformación de la UE ha estado basada en la protección de la libertad de expresión y otros derechos y libertades garantizados por la Carta de los Derechos Fundamentales de la Unión Europea. En línea con esos derechos y libertades, más que penalizar o prohibir la desinformación como tal, la estrategia de la UE tiene como objetivo hacer que el entorno digital y sus agentes sean más transparentes y responsables, haciendo que las prácticas de moderación de contenidos sean más transparentes, empoderando a los ciudadanos y fomentando un debate abierto y democrático[3]. Para tal fin, la UE ha intentado movilizar a todas las partes interesadas pertinentes, incluidas las autoridades públicas, las empresas, los medios de comunicación, las instituciones académicas y la sociedad civil.

Un elemento central de los esfuerzos de la UE ha sido el Código autorregulador de Buenas Prácticas de la Unión en materia de Desinformación[4]. En vigor desde octubre de 2018, los signatarios del Código incluyen actualmente a las principales plataformas en línea activas en la UE, así como, entre otros, a las principales asociaciones comerciales que representan al sector publicitario europeo. La Comisión considera que el Código es un logro sustancial y pionero. Ha ofrecido un instrumento innovador para garantizar una mayor transparencia y rendición de cuentas de las plataformas en línea, así como un marco estructurado para el seguimiento y mejora de las políticas de las plataformas en materia de desinformación.

No obstante, la evaluación de la Comisión del Código de Buenas Prácticas en 2020[5] ha revelado deficiencias importantes. Entre otras, una aplicación incoherente e incompleta del Código en las plataformas y los Estados miembros, limitaciones intrínsecas al carácter autorregulador del Código, así como deficiencias en cuanto a la cobertura de los compromisos del mismo. Asimismo, la evaluación puso de relieve la inexistencia de un mecanismo de seguimiento adecuado, incluido de indicadores clave de rendimiento

[1] Comunicación conjunta «La lucha contra la desinformación acerca de la COVID-19: contrastando los datos», JOIN(2020) 8 final.
[2] En el Plan de Acción contra la desinformación [JOIN(2018) 36 final], la Comisión Europea y la Alta Representante establecen una estrategia general para contrarrestar la desinformación en la UE.
[3] Aunque las condiciones de las plataformas en línea pueden abarcar también contenidos nocivos, pero no ilegales, cuando la desinformación constituye un contenido ilegal (por ejemplo, un discurso de odio o contenido terrorista), se aplican las soluciones legislativas pertinentes.
[4] https://ec.europa.eu/digital-single-market/en/code-practice-disinformation.
[5] SWD (2020) 180 final.

(KPI), la falta de compromisos sobre el acceso a los datos de las plataformas para investigar la desinformación y la participación limitada de las partes interesadas, en particular del sector publicitario. Por lo tanto, la Comisión anunció en el Plan de Acción para la Democracia Europea[6] que publicará orientaciones para reforzar el Código, como parte de las medidas generales destinadas a abordar la desinformación en el entorno digital, y que presentará una legislación específica sobre la transparencia de la publicidad política.

Para intensificar la lucha contra la desinformación, la Ley de Servicios Digitales[7] propuesta por la Comisión establece un marco corregulador a través de códigos de conducta para abordar los riesgos sistémicos vinculados a la desinformación. Además, introduce medidas de transparencia de amplio alcance en torno a la moderación de contenidos y la publicidad, y propone obligaciones jurídicas vinculantes y ejecutorias para plataformas en línea de muy gran tamaño[8] destinadas a evaluar y abordar los riesgos sistémicos para los derechos fundamentales o aquellos que plantean la manipulación deliberada de su servicio.

Las Orientaciones se basan en la experiencia de la Comisión hasta la fecha respecto al seguimiento y evaluación del Código[9] y en el informe de la Comisión sobre las elecciones de 2019[10]. Asimismo, contribuye a la respuesta de la Comisión a las conclusiones del Consejo Europeo de diciembre de 2020[11]. Para recopilar aportaciones para las Orientaciones, la Comisión organizó debates con múltiples partes interesadas[12], así como un taller para los Estados miembros.

Las presentes Orientaciones establecen las opiniones de la Comisión sobre cómo deben reforzar las plataformas y otras partes interesadas pertinentes sus medidas destinadas a abordar las deficiencias y carencias del Código y crear un entorno digital más transparente, seguro y fiable. Un ámbito concreto en el que el Código no ha logrado realizar avances suficientes es la desmonetización de la desinformación, en la que los anuncios en línea siguen incentivando la difusión de la desinformación[13]. Las plataformas

---

[6] COM (2020) 790 final.

[7] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se modifica la Directiva 2000/31/CE, COM(2020) 825 final. Las referencias a la Ley de servicios digitales en el presente documento deben entenderse como si fueran al texto propuesto por la Comisión.

[8] La propuesta de Ley de servicios digitales define las plataformas de muy gran tamaño en su artículo 25 como plataformas en línea que prestan sus servicios a un número medio mensual de destinatarios del servicio activos en la Unión correspondiente al 10 % de la población de esta.

[9] Evaluación de la Comisión de septiembre de 2020, SWD (2020) 180 final.

[10] Informe sobre las elecciones al Parlamento Europeo de 2019, SWD (2020) 113 final, https://ec.europa.eu/info/files/com_2020_252_en.pdf_en.

[11] https://www.consilium.europa.eu/media/47348/1011-12-20-euco-conclusions-es.pdf.

[12] Hay disponible un resumen de los debates con las partes interesadas en el siguiente enlace: https://digital-strategy.ec.europa.eu/en/library/summary-multi-stakeholder-discussions-preparation-guidance-strengthen-code-practice-disinformation.

[13] Los datos también muestran que los ingresos procedentes de los anuncios en línea siguen contribuyendo significativamente a la monetización de los sitios web de desinformación, incluidos los anuncios de grandes marcas colocados involuntariamente junto a los contenidos de desinformación (por ejemplo, el informe del Global Disinformation Index https://disinformationindex.org/2020/03/why-is-ad-tech-giving-millions-to-eu-disinformation-sites/ y el informe de Avaaz https://secure.avaaz.org/campaign/en/youtube_climate_misinformation/).

en línea y otros agentes del ecosistema de la publicidad en línea deben asumir la responsabilidad y trabajar juntos para suprimir la financiación de la desinformación. Además, el Código revisado debe reforzar los compromisos para limitar los comportamientos manipuladores, reforzar los instrumentos de empoderamiento de los usuarios, aumentar la transparencia de la publicidad política y seguir empoderando a la comunidad investigadora y de verificación de datos. Asimismo, las Orientaciones también establecen las piedras angulares de un marco mejorado y sólido para el seguimiento del Código reforzado. Este también debe intentar lograr una participación más amplia de nuevos signatarios, como son las plataformas en línea adicionales activas en la UE, así como otros agentes pertinentes.

Reforzar el Código ofrece inmediatamente a las partes interesadas la oportunidad de diseñar medidas adecuadas con vistas a la adopción de la propuesta de Ley de servicios digitales. En particular, las Orientaciones también pretenden desarrollar el actual Código de Buenas Prácticas para convertirlo para convertirlo en un «Código de Conducta», como se prevé en su artículo 35. Concretamente, las plataformas de muy gran tamaño[14] se beneficiarán de participar en el Código reforzado en previsión de las nuevas obligaciones que se les aplicarán en virtud de la propuesta de Ley de servicios digitales, en particular en materia de evaluación del riesgo, reducción del riesgo, empoderamiento de los usuarios y transparencia en torno a la publicidad. Las plataformas más pequeñas y otras partes interesadas también se beneficiarán de adherirse a compromisos adecuados en virtud del Código reforzado para sacar provecho de sus buenas prácticas y protegerse frente a riesgos de reputación planteados por el uso indebido de sus sistemas para propagar desinformación.

Sin perjuicio del acuerdo final de los colegisladores sobre la Ley de servicios digitales o sobre la iniciativa legislativa de la Comisión sobre la transparencia de la publicidad política, el Código de Buenas Prácticas reforzado puede servir como instrumento para que las plataformas en línea mejoren sus políticas y reduzcan los riesgos vinculados a la desinformación que sus servicios plantean para la democracia.

El refuerzo del Código no es únicamente un paso provisional. Las presentes Orientaciones instan a convertir el Código en un instrumento sólido, estable y flexible que haga a las plataformas en línea más transparentes y responsables desde el diseño.

2 SEGUIMIENTO DE LA COVID-19: RESULTADOS Y LECCIONES APRENDIDAS

Además de las lecciones aprendidas a través de la evaluación del Código de Buenas Prácticas, se han adquirido nuevas perspectivas en virtud del programa de seguimiento establecido tras la Comunicación conjunta «La lucha contra la desinformación acerca de la COVID-19: contrastando los datos»[15], durante el cual las plataformas en línea signatarias del Código han informado mensualmente de las acciones adoptadas para hacer frente a la desinformación acerca de la COVID-19 en la UE.

[14] En el sentido del artículo 25 de la Ley de servicios digitales propuesta por la Comisión. Con respecto a la definición, véase la nota a pie de página 8.
[15] Comunicación conjunta «La lucha contra la desinformación acerca de la COVID-19: contrastando los datos», JOIN(2020) 8 final.

El programa de seguimiento no solo ha ofrecido una perspectiva general exhaustiva de las acciones adoptadas para contrarrestar la desinformación en torno a la COVID-19 a partir de los compromisos del Código, sino que también ha sometido a este a una prueba de resistencia.

Los informes de las plataformas muestran que los compromisos del Código se han aplicado mediante acciones eficaces en distintos ámbitos, como una mayor visibilidad de las fuentes autorizadas en sus servicios; el desarrollo y despliegue de nuevos instrumentos y servicios para facilitar el acceso a información fiable; acciones para abordar el contenido que incluya información falsa o engañosa que pueda provocar daños físicos o afectar a la eficacia de las políticas de salud pública; prohibir expresamente la publicidad que aprovecha la crisis o propaga desinformación sobre la COVID-19.

En general, el programa ha demostrado que el Código ofrece un marco ágil y estructurado que puede desplegarse y traducirse en medidas contundentes por parte de los signatarios para luchar contra la desinformación en situaciones de crisis y que es complementario a las obligaciones derivadas de marcos reguladores aplicables. Asimismo, el Código ofrecía una estructura útil para el seguimiento de estas medidas en una situación extraordinaria, cambiando el centro de atención de forma dinámica a medida que la crisis evolucionaba (por ejemplo, para centrarse en la desinformación en torno a las vacunas de la COVID-19).

Al mismo tiempo, el programa de la COVID-19 puso de relieve una serie de deficiencias del actual marco de seguimiento del Código de Buenas Prácticas:

- *Calidad de los informes.* Existen variaciones sustanciales en la coherencia, calidad y nivel de detalle de los informes. La falta de datos suficientemente detallados, especialmente a nivel de los Estados miembros, significó que la información ofrecida no revelaba si las acciones notificadas se implementaron en todos los Estados miembros o en todas las lenguas de la UE. Además, la inexistencia de un modelo de notificación común y acordado sigue obstaculizando un seguimiento y unas comparaciones entre plataformas más eficientes.
- *Indicadores clave de rendimiento*. Aunque la calidad y el nivel de detalle de los informes mejoró con el tiempo, los datos aportados siguen sin ser adecuados y suficientemente detallados para medir hasta qué punto se aplican los compromisos o el efecto de las acciones adoptadas.
- *Evaluación independiente*. El seguimiento de la COVID-19 ha confirmado la necesidad de una verificación independiente de los informes de los signatarios, en particular, de si las políticas y acciones notificadas se han aplicado en los Estados miembros y en todas las lenguas de la UE, y si los informes abordan suficientemente los problemas de desinformación a nivel nacional[16].
- *Falta de una suficiente cobertura de verificación de datos.* Durante la «infodemia» de la COVID-19, los signatarios han aumentado sus actividades en materia de verificación de datos en sus servicios, las cuales también están cada vez más disponibles para los usuarios de aplicaciones de mensajería privada. No obstante, el contenido etiquetado como falso por verificadores de datos independientes tiende a

[16] Como se prevé en la Comunicación de junio de 2020, el Grupo de Entidades Reguladoras Europeas para los Servicios de Comunicación Audiovisual asiste a la Comisión en el programa de seguimiento de la COVID-19.

resurgir en las plataformas debido a la inexistencia de un repositorio centralizado de verificación de datos.

- *Monetización continua de la desinformación a través de colocación de anuncios.* A pesar de las medidas para limitar la monetización de la desinformación, distintas investigaciones pertinentes muestran que los problemas persisten en este ámbito[17].

3 CUESTIONES HORIZONTALES QUE DEBEN ABORDARSE

3.1 Compromisos reforzados para lograr los objetivos del Código

Los compromisos del actual Código de Buenas Prácticas no son suficientemente eficaces a la hora de ofrecer una respuesta integral al fenómeno de la desinformación. Existe la necesidad de contar con unos compromisos más sólidos y específicos en todos los ámbitos del Código para abordar las deficiencias y carencias, incluidos los riesgos nuevos y emergentes. A fin de garantizar que el Código sigue siendo un instrumento vivo, los signatarios deben establecer un mecanismo permanente para su adaptación periódica.

3.2 Ampliación del alcance

La «infodemia» en torno a la pandemia de COVID-19 ha demostrado que la información errónea[18] (información falsa o engañosa propagada sin una intención maliciosa) también puede suponer un perjuicio público sustancial si se viraliza. Aunque el principal objetivo sigue siendo la desinformación en sentido estricto[19], en el Código reforzado, los signatarios deben comprometerse a aplicar políticas adecuadas y a adoptar medidas proporcionadas para reducir los riesgos que plantea la información engañosa, en caso de que exista una importante dimensión de perjuicio público y con salvaguardias adecuadas para la libertad de palabra. Se debe empoderar a los usuarios para contrastar esta información con las fuentes autorizadas y se les debe informar en caso de que se pueda comprobar que la información que ven es falsa. De conformidad con esto, dependiendo de su carácter, no todos los compromisos del Código se aplicarán a la información engañosa.

Las presentes Orientaciones usan (para facilitar la consulta) el término general «desinformación» para referirse a los diferentes fenómenos que deben abordarse, aunque

---

[17] La investigación del Global Disinformation Index de enero y febrero de 2021 sobre Francia, Alemania, Italia y España pone de relieve que la mayoría de las empresas tecnológicas no tienen políticas específicas sobre contenidos de desinformación acerca de la COVID-19 o que dichas políticas se infringen y siguen financiando sitios señalados públicamente como proveedores de desinformación: https://disinformationindex.org/2021/02/ad-funded-covid-19-conspiracy-sites-a-look-at-the-eu/. La investigación de Avaaz de agosto de 2020 puso de relieve que se calcula que el contenido de los diez principales sitios web que propagan información sanitaria engañosa tenía casi cuatro veces tantas visitas en Facebook como el contenido equivalente de los sitios web de las diez principales instituciones sanitarias: https://secure.avaaz.org/campaign/en/facebook_threat_health/.

[18] El Plan de Acción para la Democracia Europea define la información engañosa de la siguiente manera: «la información engañosa es la información con contenidos falsos o engañosos compartida sin intención de perjudicar, aunque sus efectos pueden ser nocivos, es decir, cuando la gente comparte información falsa con amigos y familia, de buena fe».

[19] El Plan de Acción para la Democracia Europea define la desinformación de la siguiente manera: «la desinformación es un contenido falso o engañoso que se difunde con intención de engañar o de obtener una ganancia económica o política y que puede causar un perjuicio público».

reconoce claramente las importantes diferencias que existen entre ellos[20]. La desinformación en este aspecto incluye la desinformación en sentido estricto, la información engañosa, así como las operaciones de influencia en la información[21] y la injerencia extranjera[22] en el espacio de información, incluido de agentes extranjeros, en caso de que la manipulación de la información se use con el efecto de causar un importante perjuicio público.

3.3 Mayor participación

Los signatarios del actual Código incluyen a las principales plataformas en línea que operan en la UE. No obstante, una mayor participación tanto de las plataformas establecidas como de las emergentes puede ofrecer una respuesta más amplia y coordinada a la propagación de la desinformación. Los posibles nuevos signatarios pueden incluir a proveedores de servicios en línea que difunden información al público, como medios sociales o servicios de búsqueda de menor tamaño (por ejemplo, agentes que ofrecen servicios a nivel nacional o regional o de forma especializada/temática). Dadas las pertinentes cargas normativas, incluidas las obligaciones de presentación de informes, los compromisos en virtud del Código reforzado deben tener en cuenta el tamaño de los servicios de los signatarios. Mientras que las plataformas en línea de muy gran tamaño necesitarán adoptar medidas sólidas para abordar los riesgos sistémicos pertinentes en virtud de la propuesta de Ley de servicios digitales, las medidas aplicables a servicios más pequeños o emergentes no les deben imponer una carga desproporcionada.

Asimismo, los servicios de mensajería privada pueden usarse de forma indebida para alimentar la desinformación y la información engañosa, como se observó en las recientes campañas electorales y durante la pandemia de COVID-19[23]. Estos proveedores de servicios pueden ser signatarios del Código, que se comprometen a adoptar medidas específicas adecuadas para este tipo de servicios, sin un debilitamiento del cifrado usado normalmente por este tipo de servicios, y teniendo en cuenta la protección de la intimidad y el derecho a la vida privada y familiar, incluidas las comunicaciones.

A fin de aumentar la repercusión del Código sobre la desmonetización de la desinformación, resulta esencial una mayor participación de las partes interesadas del ecosistema de la publicidad más allá del círculo de los actuales signatarios del Código (asociaciones europeas y nacionales del sector de la publicidad). El Código se beneficiaría en particular de una mayor implicación de las marcas (especialmente de aquellas con un importante gasto en publicidad en línea), así como de otros participantes del sector de la publicidad en línea (por ejemplo, intercambios de publicidad, proveedores de tecnología publicitaria, agencias de comunicación) y otros agentes que

[20] En caso pertinente, las Orientaciones distinguen entre las diferentes subcategorías.
[21] Tal como se define en el Plan de Acción para la Democracia Europea: «por operación de influencia en la información se entiende los esfuerzos coordinados tanto de actores nacionales como extranjeros para influir en un público destinatario usando una serie de medios engañosos, como la supresión de fuentes de información independientes, unida a la desinformación».
[22] Tal como se define en el Plan de Acción para la Democracia Europea: «por injerencia extranjera en el espacio de información, a menudo realizada como parte de una operación híbrida más amplia, pueden entenderse los esfuerzos coercitivos y engañosos para perturbar la libre formación y manifestación de la voluntad política de las personas por parte de un actor estatal extranjero o de sus agentes».
[23] «Stop the virus of disinformation» [«Parar el virus de la desinformación», documento en inglés], Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia, http://www.unicri.it/sites/default/files/2020-11/SM%20misuse.pdf.

ofrecen servicios que pueden usarse para monetizar la desinformación (por ejemplo, servicios de pago electrónico, plataformas de comercio electrónico, sistemas de financiación participativa/donación)[24].

Entre los nuevos signatarios también se puede incluir a otras partes interesadas que pueden tener una repercusión significativa gracias a sus herramientas, instrumentos y soluciones o a su experiencia específica pertinente, incluidos verificadores de datos, organizaciones que ofrecen calificaciones relacionadas con los sitios de desinformación o que evalúan la desinformación, así como proveedores de soluciones tecnológicas que pueden apoyar los esfuerzos para abordar la desinformación. Estas organizaciones pueden contribuir de forma considerable a una aplicación eficaz del Código y al éxito de este.

3.4 Compromisos específicos

Para facilitar una mayor participación, el Código reforzado debe incluir compromisos específicos que se correspondan con la diversidad de servicios ofrecidos por los signatarios y las funciones concretas que desempeñan en el ecosistema.

Los signatarios deben adherirse a los compromisos que resultan pertinentes para sus servicios. Aunque la participación en el Código y la adhesión a sus compromisos siguen siendo voluntarias, a fin de garantizar la eficacia del Código como herramienta de reducción del riesgo, los signatarios no deben renunciar, en principio, a los compromisos que resultan pertinentes para sus servicios. Cuando los signatarios renuncien a adherirse a un compromiso concreto que resulte pertinente para sus servicios, deben ofrecer una justificación pública, a tenor del considerando 68 de la propuesta de Ley de servicios digitales. Los signatarios que ofrecen herramientas, instrumentos o soluciones para luchar contra la desinformación pueden adherirse a compromisos adecuados y apoyar a otros signatarios del Código con su experiencia. Cualquier requisito de presentación de informes para dichas organizaciones debe adaptarse a su misión.

3.5 Observatorio Europeo de los Medios Digitales

A fin de ofrecer una contribución eficaz para abordar la cuestión de la desinformación, resulta esencial contar con el apoyo de una comunidad multidisciplinar, incluidos verificadores de datos, investigadores del mundo académico y otras partes interesadas pertinentes. Para contribuir a la creación de dicha comunidad y facilitar su labor, se creó el Observatorio Europeo de los Medios Digitales (EDMO)[25]. Al ofrecer apoyo a investigadores y verificadores de datos independientes, el EDMO y sus centros nacionales aumentarán su capacidad para detectar y analizar campañas de desinformación. El EDMO puede desempeñar una función importante a la hora de lograr varios de los objetivos del Código. Por tanto, se espera que los signatarios del mismo cooperen con el Observatorio según proceda.

---

[24] «How COVID-19 conspiracists and extremists use crowdfunding platforms to fund their activities» [«Cómo los conspiradores y extremistas de la COVID-19 usan las plataformas de financiación participativa para financiar sus actividades», documento en inglés], EUDisinfoLab https://www.disinfo.eu/publications/how-covid-19-conspiracists-and-extremists-use-crowdfunding-platforms-to-fund-their-activities/.

[25] https://edmo.eu/.

3.6 Sistema de Alerta Rápida

Como se describe en el Plan de Acción contra la desinformación de 2018[26], las plataformas en línea deben cooperar con el Sistema de Alerta Rápida de la UE, que conecta a todos los Estados miembros de la UE y las instituciones de la UE pertinentes para poder ofrecer respuestas conjuntas a la desinformación intercambiando información y ofreciendo alertas de forma oportuna sobre campañas de desinformación. A partir de esto, el Código reforzado debe explorar las oportunidades para reforzar dicha cooperación, en particular facilitando un intercambio informal entre los signatarios para presentar su trabajo y conclusiones, así como para garantizar unos vínculos estrechos, simplificados y coherentes a nivel nacional entre todos los Estados miembros y los signatarios según proceda. Este también debe tener en cuenta la cooperación con el EDMO, como se ha mencionado anteriormente.

4 ANÁLISIS DE LA COLOCACIÓN DE ANUNCIOS

Como se ha explicado, las medidas contundentes para desmonetizar a los proveedores de desinformación resultan esenciales para el éxito del Código. Por lo tanto, los compromisos del Código reforzado deben adoptar medidas más detalladas y específicas para abordar los riesgos de la desinformación vinculados a la distribución de publicidad en línea, teniendo en cuenta los futuros requisitos normativos de la propuesta de Ley de servicios digitales aplicables a toda la publicidad en línea, incluida la publicidad política y temática y, en la medida de lo posible, la iniciativa anunciada sobre publicidad política.

4.1 Desmonetización de la desinformación

El Código debe reforzar los compromisos destinados a suprimir la financiación de la difusión de desinformación en los propios servicios de los signatarios o en sitios web de terceras partes[27]. Para mejorar la transparencia y la rendición de cuentas en torno a la colocación de anuncios, los signatarios que participen en ella, incluidas las empresas de tecnología publicitaria[28], deben identificar los criterios que usan para colocar los anuncios, y adoptar medidas que permitan verificar el lugar de aterrizaje/destino de los anuncios, con el objetivo de evitar la colocación de estos junto a contenidos de desinformación o en lugares conocidos por publicar desinformación de forma reiterada. Las plataformas deben comprometerse, en particular, a endurecer los requisitos de admisibilidad y los procesos de revisión de contenidos para la monetización de contenidos y los programas de reparto de los ingresos por publicidad en sus servicios para impedir la participación de agentes que publican sistemáticamente contenidos desacreditados como desinformación[29]. Además, las plataformas también deben comprometerse a reforzar las políticas pertinentes y a ejercer la diligencia debida con

---

[26] JOIN(2018) 36 final.

[27] Las pruebas también muestran que los ingresos procedentes de los anuncios en línea siguen contribuyendo significativamente a la monetización de los sitios web de desinformación, incluidos los anuncios de grandes marcas colocados involuntariamente junto a los contenidos de desinformación. Por ejemplo, el Global Disinformation Index calcula que alrededor de 76 millones USD al año en ingresos por publicidad circulan hasta sitios de desinformación dirigidos a Europa: https://disinformationindex.org/2020/03/why-is-ad-tech-giving-millions-to-eu-disinformation-sites/.

[28] Un número limitado de empresas de tecnología publicitaria ya han adoptado dichas políticas.

[29] Véase, por ejemplo, el informe de Avaaz de 2020, «Why is YouTube Broadcasting Climate Misinformation to Millions?» [«¿Por qué Youtube emite desinformación climática para millones de personas?», documento en inglés]: https://secure.avaaz.org/campaign/en/youtube_climate_misinformation/.

vistas a excluir la participación en las redes de publicidad o en los intercambios de publicidad de sitios web que provean constantemente contenidos de desinformación.

Asimismo, los compromisos en este ámbito deben basarse en la disponibilidad y adopción de instrumentos de seguridad de marcas, así como mejorarlos, y estos deben integrar información y análisis de verificadores de datos, investigadores y otras partes interesadas pertinentes que ofrecen información, por ejemplo, sobre las fuentes de las campañas de desinformación. Con el apoyo de esta información e instrumentos, los propietarios de las marcas y otros anunciantes deben comprometerse a hacer todo lo posible por evitar la colocación de sus anuncios junto a contenidos de desinformación o en lugares que publican desinformación de forma reiterada.

4.2 Mejorar de la cooperación entre los agentes pertinentes

Lograr unos resultados tangibles exige una estrecha cooperación de los diferentes agentes del ecosistema de la publicidad. Para tal fin como se establece en la sección 3.3, resulta esencial una mayor participación de las partes interesadas de dicho ecosistema. El Código reforzado debe ofrecer un marco para esta participación ampliada que refuerce la cooperación de todos los agentes pertinentes y siga facilitando las iniciativas intersectoriales en curso en este ámbito[30].

Como parte del Código reforzado, todos los agentes implicados en la compra, venta y colocación de anuncios digitales deben comprometerse a intercambiar mejores prácticas y a reforzar la cooperación. Dicha cooperación debe facilitar la integración y el flujo de información en toda la cadena de valor de la publicidad, en particular la información pertinente para identificar a proveedores de desinformación respetando plenamente todas las normas pertinentes en materia de protección de datos.

La cooperación entre plataformas también puede incluir el intercambio de información sobre anuncios de desinformación rechazados por una de ellas para impedir su aparición en el resto (por ejemplo, mediante la creación de un repositorio común de anuncios rechazados), con el objetivo de informar a estas últimas, cuyos servicios también puedan verse afectados.

Las acciones para suprimir la financiación de la desinformación deben ampliarse mediante la participación de agentes activos en la cadena de valor de la monetización en línea, como los servicios de pago electrónico en línea, las plataformas de comercio electrónico y los sistemas de financiación participativa/donación pertinentes.

[30] La Global Alliance for Responsible Media, lanzada en junio de 2019 bajo los auspicios de la Federación Mundial de Anunciantes, incluye signatarios del Código de las plataformas y del sector de la publicidad, así como otras partes interesadas destacadas del ecosistema de la publicidad. Está desarrollando un conjunto de definiciones y estándares comunes para toda la industria sobre cómo se clasifica el contenido nocivo en las plataformas, cómo se aprueba por parte de los anunciantes y cómo se aplica por parte de las plataformas en sus productos anunciados e instrumentos de seguridad de marcas. En particular, la Alliance busca incluir en dicho conjunto una categoría independiente para la desinformación y la información engañosa. Véase el documento «Interim Report on Activities related to the EU Code of Practice on Disinformation» [«Informe provisional sobre las actividades relacionadas con el Código de Buenas Prácticas de la Unión en materia de Desinformación», documento en inglés] de la Federación Mundial de Anunciantes, septiembre de 2020, p. 2: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69683.

4.3 Compromisos para abordar la publicidad con contenidos de desinformación

En virtud del Código reforzado, los signatarios deben comprometerse a designar políticas adecuadas y específicas en materia de publicidad que aborden el uso indebido de sus sistemas para propagar desinformación[31]. Deben reforzar estas políticas de forma coherente y eficaz. Para tal fin, los signatarios deben cooperar con los verificadores de datos para identificar anuncios que contengan desinformación que haya sido verificada y desacreditada. Para garantizar una aplicación coherente, los signatarios deben comprometerse a adaptar sus actuales sistemas de verificación y revisión de anuncios para garantizar que los anuncios que se colocan a través de sus servicios o en estos cumplen sus políticas en materia de publicidad respecto a la desinformación. Asimismo, los signatarios deben comprometerse a explicar claramente a los anunciantes qué políticas en materia de publicidad se han infringido cuando rechacen o eliminen anuncios de desinformación o desactiven cuentas publicitarias[32].

5 PUBLICIDAD POLÍTICA Y PUBLICIDAD TEMÁTICA

La «publicidad política» y la «publicidad temática»[33] desempeñan una función importante a la hora de configurar las campañas políticas y los debates públicos en torno a temas sociales clave. Dicho contenido de pago en línea puede tener un papel decisivo en la formación de la opinión pública e influir en el resultado de las elecciones. La organización de las elecciones en la UE está ampliamente regulada a nivel de los Estados miembros, con diferentes normas pertinentes que afectan a la publicidad política, incluida su transparencia. En el Plan de Acción para la Democracia Europea, la Comisión anunció la adopción de medidas legislativas para reforzar la transparencia de la publicidad política. Para garantizar un nivel adecuado de transparencia y rendición de cuentas en este ámbito, los compromisos del Código deben seguir reforzándose, en apoyo de un marco jurídico más amplio.

La revisión del Código en este ámbito deberá tener en cuenta la futura propuesta legislativa de la Comisión sobre la transparencia del contenido político patrocinado y las disposiciones pertinentes de la propuesta de Ley de servicios digitales. Un Código reforzado será un vehículo importante para lograr un avance tangible con el fin de apoyar el actual marco jurídico, así como para allanar el camino hacia una legislación reforzada y a través del nuevo marco legislativo una vez adoptado, así como para diseñar soluciones impulsadas por el sector para apoyar su aplicación y lograr un progreso continuo en este ámbito.

---

[31] Los datos muestran la persistencia de los anuncios en línea con contenidos de desinformación que los verificadores de datos han identificado y desacreditado. Véase «Facebook Approved Ads With Coronavirus Misinformation» [«Anuncios aprobados por Facebook con desinformación sobre el coronavirus», documento en inglés]: https://www.consumerreports.org/social-media/facebook-approved-ads-with-coronavirus-misinformation/.

[32] Como ha señalado la Comisión, las políticas de las plataformas persiguen una serie de objetivos, algunos de los cuales no están específicamente adaptados para abordar la desinformación (por ejemplo, demandas mercantiles sin fundamento, prácticas comerciales engañosas). Véase el documento SWD(2020) 180 final.

[33] Aunque actualmente no existe una definición común de los anuncios temáticos en el Código, parece existir el acuerdo de que son anuncios que incluyen contenido patrocinado sobre temas sociales o relacionados con un debate de interés general que pueden tener una gran repercusión sobre el discurso público. Algunos ejemplos de esos temas son el cambio climático, los problemas medioambientales, la inmigración o la COVID-19.

Para una aplicación coherente y eficaz de los compromisos, se necesita un entendimiento común entre los signatarios de la «publicidad política» y la «publicidad temática» que tenga en cuenta de forma adecuada los actuales marcos jurídicos nacionales aplicables. Los signatarios deben garantizar que cumplen las leyes aplicables y que ajustan sus prácticas a la futura legislación sobre la transparencia del contenido político patrocinado.

5.1 Etiquetado eficiente de los anuncios políticos y temáticos

El Código debe incluir unos compromisos reforzados que garanticen la transparencia y divulgación pública de los anuncios políticos y temáticos, teniendo en cuenta las disposiciones pertinentes de la propuesta de Ley de servicios digitales[34], la futura iniciativa legislativa sobre la transparencia de la publicidad política y sin perjuicio de los actuales marcos reguladores. Estos anuncios deben estar etiquetados de forma clara y eficaz, se les debe distinguir como contenido de pago y los usuarios deben poder entender que los contenidos presentados contienen publicidad relacionada con temas políticos o sociales. El Código reforzado puede incluir una serie de criterios y ejemplos comunes sobre el marcado y etiquetado de los anuncios políticos y temáticos. Cuando proceda, los signatarios deben integrar investigaciones pertinentes para mejorar la eficacia de las etiquetas a la hora de informar a los usuarios[35]. El Código debe incluir compromisos destinados a garantizar que las etiquetas sigan en su lugar cuando los usuarios compartan los anuncios políticos o temáticos de forma orgánica[36], de forma que sigan siendo claramente identificados como anuncios.

5.2 Compromisos de verificación y transparencia para los anuncios políticos y temáticos

Los signatarios que presenten anuncios políticos y temáticos deben garantizar que la identidad de los anunciantes sea visible para los usuarios, incluido un compromiso específico que establezca obligaciones de transparencia de conformidad con los requisitos de la propuesta de Ley de servicios digitales[37].

Asimismo, los signatarios deben hacer un esfuerzo razonable para garantizar, a través de unos sistemas eficaces de verificación y autorización de identidad, que se cumplen todas las condiciones necesarias antes de permitir la colocación de estos tipos de anuncios.

5.3 Transparencia en las plataformas de mensajería

El Código de Buenas Prácticas revisado debe incluir nuevos compromisos específicos que aborden el uso de plataformas de mensajería para la difusión de anuncios políticos y temáticos, respectando plenamente el Reglamento General de Protección de Datos (RGPD) y los requisitos de la UE en materia de intimidad en los servicios de comunicaciones electrónicas. El mencionado requisito relativo a que el contenido político patrocinado que comparten los usuarios debe seguir etiquetándose como

---

[34] El artículo 24 en particular.

[35] Dobber *et al.*: «Effectiveness of online political ad disclosure labels: empirical findings» [«Eficacia de las etiquetas de divulgación de anuncios políticos en línea: conclusiones empíricas», documento en inglés], marzo de 2021: https://www.uva-icds.net/wp-content/uploads/2021/03/Summary-transparency-discloures-experiment_update.pdf.

[36] El contenido orgánico es contenido gratuito que los usuarios comparten mutuamente sin pagar por él. Incluye también situaciones en las que los usuarios comparten mutuamente contenidos patrocinados que, a continuación, se convierten en contenido orgánico.

[37] Propuesta de Ley de servicios digitales, artículo 30.

contenido de pago debe aplicarse en la medida de lo posible al contenido político patrocinado compartido a través de las plataformas de mensajería. Para tal fin, los signatarios deben desarrollar soluciones que sean compatibles con la tecnología de cifrado que suelen usar las plataformas de mensajería, sin un debilitamiento del cifrado.

5.4 Segmentación de los anuncios políticos

La microsegmentación de la publicidad política puede plantear diferentes problemas. Plantea problemas de cumplimiento de las normas de protección de datos, ya que la microsegmentación se basa en información personal y, a veces, incluye técnicas sofisticadas de elaboración de perfiles psicológicos[38]. Puede afectar al derecho de los votantes a recibir información, ya que la microsegmentación permite a los anunciantes de contenidos políticos enviar mensajes adaptados a públicos destinatarios, mientras que se puede privar a otros públicos de esta información. La microsegmentación dificulta la verificación de datos o el escrutinio de dichos anuncios, así como que las personas puedan hacer valer sus derechos, incluidos los relativos a la protección de datos. A su vez, esto puede aumentar el riesgo de polarización política[39].

El Código reforzado debe contribuir a limitar o evitar los riesgos asociados a la microsegmentación de las personas con la publicidad política o temática. En este sentido, se debe garantizar el pleno cumplimiento del RGPD y de otras leyes pertinentes, en particular obteniendo un consentimiento válido en caso necesario[40]. Debe facilitarse el acceso a la información para permitir a las autoridades competentes desempeñar su función de seguimiento y de control del cumplimiento de la normativa.

Los signatarios deben comprometerse a garantizar que los ciudadanos son claramente informados cuando se les aplica la microsegmentación y que se les ofrece información significativa sobre los criterios y datos utilizados para este fin. Deben aplicar medidas sólidas relacionadas con la transparencia, incluidas bibliotecas de anuncios consultables específicas con todos los anuncios microsegmentados presentados para grupos de usuarios concretos[41], acompañadas de información sobre criterios de segmentación y entrega.

---

[38] La propuesta de Ley de servicios digitales y la propuesta de Ley de Mercados Digitales incluyen obligaciones de transparencia específicas.

[39] Véase, por ejemplo, Papakyriakopoulos *et. al*: «Social media and microtargeting: Political data processing and the consequences for Germany» [«Medios sociales y microsegmentación: tratamiento de datos políticos y consecuencias para Alemania», documento en inglés], Big Data & Society, noviembre de 2018, doi 10.1177/2053951718811844, o Lewandowsky *et al.*: «Understanding the influence of online technologies on political behaviour and decision-making» [«Comprender la influencia de las tecnologías en línea en el comportamiento y la toma de decisiones políticos», documento en inglés], EUR 30422 EN, Oficina de Publicaciones de la Unión Europea, Luxemburgo.

[40] Para más información, véanse las Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 y las «Guidelines 08/2020 on the targeting of social media users» [«Directrices 08/2020 sobre la selección de los usuarios de los medios sociales», documento en inglés] del Comité Europeo de Protección de Datos, que ofrecen ejemplos sobre cuándo se exige el consentimiento para la publicidad personalizada.

[41] Por ejemplo, las bibliotecas de anuncios, en caso de contar con los datos necesarios, pueden usarse para verificar que existe la misma exposición temporal en línea a los mensajes políticos.

5.5 Mejora de los repositorios de anuncios y funcionalidades mínimas para las interfaces de programación de aplicaciones (API)

El Código reforzado debe garantizar que las plataformas signatarias se comprometan a mejorar la exhaustividad y la calidad de la información de sus repositorios de anuncios políticos, de forma que estos contengan de forma eficaz todos los contenidos políticos patrocinados presentados. Estos repositorios deben ofrecer información actual y actualizada periódicamente sobre el volumen y el presupuesto de los anuncios políticos presentados por los anunciantes políticos en los Estados miembros, el número de veces que se ha presentado en línea cada anuncio y los criterios de segmentación usados por el anunciante, teniendo en cuenta las disposiciones pertinentes de la propuesta de Ley de servicios digitales y de la futura propuesta legislativa sobre publicidad política[42].

Algunas plataformas han desarrollado interfaces de programación de aplicaciones (API) u otras interfaces que permiten a los usuarios e investigadores realizar búsquedas personalizadas en sus repositorios de anuncios políticos. No obstante, las funcionalidades de estas API son muy limitadas. El Código reforzado debe garantizar que las API para los repositorios de anuncios políticos de las plataformas incluyan un grupo de funcionalidades mínimas, así como un conjunto de criterios de búsqueda mínimos que permitan a los usuarios e investigadores realizar búsquedas personalizadas para recuperar datos en tiempo real en formatos estándar, así como una fácil comparación, investigación y seguimiento entre plataformas. Si se crean repositorios de anuncios temáticos, estos deben contar con funcionalidades API y capacidades de búsqueda comparables. Los compromisos también deben garantizar el amplio acceso a las API y que las funcionalidades de estas se actualicen periódicamente para satisfacer las necesidades de los investigadores.

6 INTEGRIDAD DE LOS SERVICIOS

El Código reforzado debe ofrecer una cobertura exhaustiva de las formas actuales y emergentes de comportamientos manipuladores usados para propagar la desinformación. Debe tener en cuenta el carácter evolutivo de la propagación de desinformación y los mayores riesgos asociados a esta, por ejemplo, el hecho de que las campañas de desinformación puedan formar parte de amenazas híbridas a la seguridad, concretamente en combinación con ciberataques[43]. Debe incluir compromisos específicos para abordar las vulnerabilidades y garantizar la transparencia y la rendición de cuentas respecto a las medidas adoptadas por los signatarios para limitar los comportamientos manipuladores que, según sus condiciones de servicio pertinentes, no están permitidos en los servicios de los signatarios, habida cuenta también de los futuros requisitos normativos establecidos en la propuesta de Ley de servicios digitales[44].

6.1 Entendimiento común de los comportamientos manipuladores inadmisibles

Para asegurar un enfoque coherente, el Código reforzado debe garantizar que los signatarios acuerden un entendimiento entre servicios de los comportamientos

[42] Véase la Propuesta de Ley de servicios digitales, artículo 30.
[43] Comunicación conjunta «Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas», JOIN(2018) 16 final.
[44] El artículo 26, apartado 1, letra c), de la propuesta de Ley de servicios digitales identifica la «manipulación deliberada» de los servicios como un riesgo sistémico frente al cual las plataformas de muy gran tamaño deben adoptar medidas de mitigación de riesgos.

manipuladores no permitidos en sus servicios, incluidos los «comportamientos dolosos», sin perjuicio de las leyes de la UE y nacionales existentes. Este entendimiento debe ser suficientemente amplio para abarcar todo el abanico de comportamientos que pueden usar los agentes malintencionados para intentar manipular los servicios. Para tal fin, los signatarios deben elaborar una lista exhaustiva de tácticas, técnicas y procedimientos (TTP) manipuladores que constituyen comportamientos dolosos inadmisibles en sus servicios. Las técnicas identificadas deben estar suficientemente definidas para permitir comparaciones de la prevalencia de comportamientos inadmisibles en las plataformas, así como la eficacia de las medidas adoptadas para luchar contra ellos. El entendimiento común debe ofrecer un vocabulario compartido para los signatarios, reguladores, sociedad civil y otras partes interesadas para debatir los problemas de desinformación y manipulación en línea tanto en el contexto del Código de Buenas Prácticas como en otros foros, como el Sistema De Alerta Rápida de la UE y la red de cooperación en materia de elecciones, y en preparación de la aplicación de la propuesta de Ley de servicios digitales propuesta. Este trabajo debe tener en cuenta la situación rápidamente cambiante relativa a los TTP y reflejar estos posibles cambios a la hora de desarrollar la terminología y las definiciones.

6.2 Compromisos reforzados para limitar los comportamientos manipuladores inadmisibles

El Código reforzado debe establecer nuevos compromisos en el ámbito de los comportamientos manipuladores inadmisibles, que abarquen todo el abanico de técnicas manipuladoras y que exijan respuestas eficaces para luchar contra ellos. Los compromisos deben exigir a los signatarios que aborden las técnicas manipuladoras en evolución, como las operaciones de pirateo y filtración, la apropiación de cuentas, la creación de grupos falsos, la suplantación de identidad, los *deepfakes*, la compra de participaciones falsas o la implicación opaca de personas influyentes. Además, los compromisos no deben exigir a los signatarios únicamente que publiquen políticas pertinentes, sino que también establezcan elementos, objetivos e indicadores de referencia para las medidas desplegadas para luchar contra los comportamientos manipuladores inadmisibles. El Código reforzado debe tener en cuenta las obligaciones de transparencia para los sistemas de IA que generan o manipulan contenidos, así como la lista de prácticas manipuladoras prohibidas en virtud de la propuesta de Ley sobre inteligencia artificial[45].

6.3 Ajuste de los compromisos, la cooperación y la transparencia

Para garantizar su constante pertinencia y adecuación, el Código reforzado debe establecer un mecanismo a través del cual sus compromisos puedan ajustarse a lo largo del tiempo teniendo en cuenta los datos más recientes sobre las conductas y los TTP empleados por los agentes malintencionados.

Los signatarios deben comprometerse a establecer canales de intercambio entre sus respectivos equipos de confianza y ciberseguridad y seguridad. Estos canales deben facilitar el intercambio proactivo de información sobre operaciones de influencia y la injerencia extranjera en el espacio de información en los servicios de los signatarios para evitar el resurgimiento de dichas campañas en otras plataformas. Los resultados y las lecciones aprendidas deben incluirse en los informes anuales de seguimiento de los

[45] COM (2021) 206 final.

signatarios, debatirse en el grupo de trabajo permanente[46] y ponerse a disposición de forma periódica en formatos comunes de datos[47].

Los compromisos garantizarán que todas las políticas y medidas se comuniquen claramente a los usuarios, como son a través del centro de transparencia[48]. Asimismo, los signatarios deben comprometerse a que todas las acciones contra los comportamientos manipuladores inadmisibles estén sujetas a un sistema interno de gestión de reclamaciones, teniendo en cuenta las disposiciones pertinentes de la propuesta de Ley de servicios digitales[49].

7 EMPODERAMIENTO DE LOS USUARIOS

Empoderar a los usuarios resulta esencial para limitar el impacto de la desinformación. Un mejor entendimiento del funcionamiento de los servicios en línea, así como herramientas que fomenten un comportamiento en línea más responsable o que permitan a los usuarios detectar contenidos falsos o engañosos e informar acerca de ellos, pueden limitar drásticamente la propagación de la desinformación. Los compromisos del Código en este ámbito deben ampliarse para abarcar un amplio abanico de servicios, incluidos, por ejemplo, compromisos específicos para los servicios de mensajería. Asimismo, deben incluir mecanismos para recurrir contra las medidas adoptadas por los signatarios como seguimiento a los informes de los usuarios. Los signatarios también deben considerar de forma específica la situación de los niños, los cuales pueden resultar especialmente vulnerables ante la desinformación.

7.1 Compromiso con las medidas para mejorar la alfabetización mediática

Varios signatarios han realizado esfuerzos en el ámbito de la alfabetización mediática ofreciendo a los usuarios herramientas pertinentes. En virtud del Código reforzado, los signatarios deben comprometerse a seguir realizando estos esfuerzos y especialmente a lograr una mayor participación de la comunidad de la alfabetización mediática en el diseño y aplicación de las herramientas para las campañas de alfabetización mediática y la evaluación de estas últimas en sus servicios, entre otras cosas para proteger a los niños. Estos esfuerzos también pueden estar en consonancia con las iniciativas de la Comisión en el ámbito de la alfabetización mediática[50], incluido el nuevo Plan de Acción de Educación Digital (2021-2027)[51], para aprovechar las sinergias pertinentes. Para tal fin, el Grupo de Expertos en Alfabetización Mediática de la Comisión[52] y el EDMO puede ofrecer ayuda para establecer un marco permanente de debate.

---

[46] Respecto al grupo de trabajo permanente, véase la sección 9.2.3 más adelante.
[47] Esto debe tener en cuenta también el marco AMITT (Desinformación Publicitaria y Tácticas y Técnicas de Influencia): https://cogsec-collab.org/.
[48] Respecto al centro de transparencia, véase la sección 9.2.2 más adelante.
[49] En particular, el artículo 17, que ya se aplica a decisiones incompatibles con sus condiciones, incluidas las decisiones para retirar o inhabilitar el acceso a contenidos, suspender o cesar la prestación del servicio, en todo o en parte, a los destinatarios o las decisiones de suspender o eliminar la cuenta de los destinatarios.
[50] Véanse en particular las medidas establecidas en el Plan de Acción para la Democracia Europea [COM (2020) 790 final] y el Plan de Acción para los Medios de Comunicación y Audiovisuales [COM (2020) 784 final].
[51] El Plan de Acción de Educación Digital [COM (2020) 624 final] plantea una propuesta para desarrollar unas directrices para profesores y educadores con vistas a abordar la desinformación y fomentar la alfabetización digital a través de la educación y la formación.
[52] https://digital-strategy.ec.europa.eu/en/policies/media-literacy.

7.2 Compromiso con el «diseño seguro»

El diseño y la arquitectura de los servicios en línea tienen un impacto significativo sobre el comportamiento de los usuarios[53]. Por lo tanto, los signatarios deben comprometerse a evaluar los riesgos que plantean sus sistemas y diseñar la arquitectura de sus servicios de una forma que minimice los riesgos vinculados[54] a la propagación y amplificación de la desinformación[55]. Esto también puede incluir poner a prueba previamente la arquitectura de los sistemas. Asimismo, los signatarios deben invertir en investigación y desarrollar características y diseños de productos que mejoren el pensamiento crítico de los usuarios, así como el uso responsable y seguro de sus servicios.

Las plataformas en línea también pueden colaborar con los proveedores de soluciones tecnológicas para integrar en sus servicios soluciones que permitan comprobar la autenticidad o precisión o identificar la procedencia o fuente del contenido digital[56].

Los proveedores de sistemas en línea basados en la IA también deben tener en cuenta las disposiciones pertinentes de la propuesta de Ley sobre inteligencia artificial.

7.3 Rendición de cuentas de los sistemas de recomendación

Al determinar el orden en el que se presenta la información, los sistemas de recomendación tienen una repercusión significativa sobre la información a la que realmente acceden los usuarios. Resulta de vital importancia que los signatarios del Código reforzado se comprometan a hacer que sus sistemas de recomendación sean transparentes en cuanto a los criterios usados para dar o quitar prioridad a la información, ofreciendo a los usuarios la opción de personalizar los algoritmos de clasificación. Todo esto debe hacerse respetando el principio de libertad de los medios de comunicación teniendo en cuenta los requisitos de las disposiciones pertinentes de la propuesta de Ley de servicios digitales[57].

Los compromisos también deben incluir medidas concretas para reducir los riesgos de los sistemas de recomendación que alimentan la propagación viral de la desinformación, como la exclusión del contenido recomendado de información falsa o engañosa cuando

---

[53] Véase, por ejemplo, Lewandowsky *et al.*: «Understanding the influence of online technologies on political behaviour and decision-making» [«Comprender la influencia de las tecnologías en línea en el comportamiento y la toma de decisiones políticos», documento en inglés], EUR 30422 EN, Oficina de Publicaciones de la Unión Europea, Luxemburgo 2020.

[54] Véase la propuesta de Ley de servicios digitales, artículo 26, apartado 1, letra c), sobre la evaluación de riesgos relacionada.

[55] Unas sencillas intervenciones técnicas (por ejemplo, mensajes emergentes preguntando a los usuarios si realmente desean compartir vínculos que no han visitado) pueden incitar a los usuarios a examinar el contenido antes de difundirlo, ayudando de esta forma a limitar la propagación de información falsa o engañosa por parte de usuarios que actúan de buena fe. Ejemplos: Notificación «Compruébalo antes de twittearlo» aplicada por Twitter: https://help.twitter.com/es/using-twitter/how-to-retweet;
Paneles informativos de verificación de datos de Youtube: https://support.google.com/youtube/answer/9229632?hl=es; Aviso emergente de Facebook antes de compartir contenido desacreditado por un verificador de datos: https://www.facebook.com/journalismproject/programs/third-party-fact-checking/faqs;
«Know your Facts tool» de TikTok: https://newsroom.tiktok.com/en-gb/taking-action-against-covid-19-vaccine-misinformation.

[56] En la sección 3.3, las Orientaciones invitan a las partes interesadas que puedan contribuir a través de sus herramientas, instrumentos o soluciones para luchar contra la desinformación a convertirse en nuevos signatarios del Código.

[57] A saber, los artículos 26, 27 y 29.

esta ha sido desacreditada por verificadores de datos independientes, así como de páginas web y de agentes que propagan desinformación constantemente.

7.4 Visibilidad de la información fiable de interés público

La pandemia de COVID-19 ha puesto de relieve la importancia, especialmente en tiempos de crisis, de fomentar información de interés público que sea fiable, como la ofrecida por las autoridades sanitarias en relación con las medidas que previenen la enfermedad o con la seguridad de las vacunas[58]. Los signatarios aplicaron varias soluciones para ofrecer a los usuarios dicha información, hacerla visible y facilitar el acceso a ella. A partir de esta experiencia, los signatarios del Código reforzado deben comprometerse a seguir desarrollando y aplicando herramientas específicas (por ejemplo, paneles informativos, *banners*, mensajes emergentes, mapas y notificaciones) que prioricen las fuentes autorizadas sobre temas de especial interés público y social o en situaciones de crisis, y que lleven a los usuarios hasta ellas.

Para profundizar en el actual compromiso del Código[59] sobre la priorización de contenidos pertinentes, auténticos y autorizados, los signatarios también deben comprometerse a publicar información que describa la metodología que emplean sus sistemas de recomendación en este sentido. Dicha información debe incluirse en el centro de transparencia. Los signatarios del Código deben considerar la posibilidad de garantizar que esta información pueda ser verificada por terceras partes o a través de una auditoría independiente, teniendo en cuenta también las disposiciones pertinentes de la propuesta de Ley de servicios digitales.

7.5 Advertencias dirigidas a los usuarios que interactúan o han interactuado con contenidos falsos o engañosos

El descrédito de información falsa o engañosa resulta esencial para frenar el fenómeno de la desinformación[60]. Varios signatarios han establecido una cooperación con verificadores de datos independientes o han creado equipos internos de moderación para asignar etiquetas de contenidos falsos o engañosos. No obstante, en la actualidad el Código no incluye compromisos pertinentes. Por consiguiente (complementando los nuevos compromisos para garantizar una aplicación coherente de la verificación de datos, como se analiza más adelante en la sección 8.3), los signatarios deben comprometerse a facilitar, para todas las lenguas de la UE en las que ofrezcan sus servicios, sistemas para el etiquetado periódico y coherente de los contenidos identificados como falsos o engañosos y para emitir advertencias dirigidas a usuarios que han interactuado con dichos contenidos. Los signatarios deben comprometerse a informar a los usuarios del motivo por el que ciertos contenidos o cuentas han sido etiquetados, relegados o, por el contrario, se han visto afectados por las medidas adoptadas, así como del fundamento de dicha acción. Los signatarios deben comprometerse a diseñar sus sistemas de etiquetado y advertencia de conformidad con los datos científicos actualizados sobre cómo

[58] Los informes de seguimiento de la COVID-19 ofrecen datos sobre visitas o frecuencias de clics de paneles informativos y *banners* que ofrecen dicha información: https://digital-strategy.ec.europa.eu/en/library/reports-march-actions-fighting-covid-19-disinformation-monitoring-programme.
[59] Véase el compromiso n.º 8 del Código de Buenas Prácticas en materia de Desinformación.
[60] The Debunking Handbook 2020: https://sks.to/db2020.

maximizar los efectos de dichas intervenciones, garantizando en particular que están diseñadas para captar la atención de los usuarios[61].

7.6 Funcionalidad para señalar información falsa nociva

Aunque algunos signatarios ya ofrecen una funcionalidad específica para que los usuarios señalen información falsa o engañosa, esta característica aún no está disponible en todos los servicios. El Código reforzado debe contener un compromiso específico que exija que los signatarios correspondientes ofrezcan unos procedimientos fáciles de usar y eficaces en sus servicios, permitiendo a los usuarios señalar la desinformación que pueda causar un perjuicio público o individual. Esta funcionalidad también debe servir de apoyo a los sistemas y mecanismos de etiquetado para ayudar a identificar contenidos de información falsa que resurgen tras haber sido etiquetados como falsos en otras lenguas o en otros servicios, respetando plenamente la libertad de expresión. El compromiso debe especificar que la funcionalidad debe protegerse debidamente frente a los abusos (es decir, la táctica conocida como *mass-flagging* destinada a silenciar otras voces) y estar disponible en todas las lenguas de los Estados miembros en los que se ofrecen sus servicios. Las acciones adoptadas por los signatarios respecto a los contenidos señalados deben respetar la libertad de expresión y no ser desproporcionadas. Las medidas en este ámbito pueden incluir la aplicación de un procedimiento transparente de verificación de datos al contenido señalado, junto a acciones posteriores de seguimiento, como el etiquetado del contenido cuando proceda. Los signatarios deben comprometerse a ofrecer a los usuarios información de seguimiento sobre el contenido notificado como, por ejemplo, si el contenido ha sido revisado y, en caso afirmativo, los resultados de la evaluación y cualquier acción adoptada respecto al contenido. Se debe informar igualmente a los usuarios cuyo contenido o cuentas hayan sido sometidas a dichas medidas para que entiendan los motivos subyacentes a las acciones adoptadas y puedan acceder a un mecanismo adecuado y transparente para recurrir y buscar reparación por las medidas aplicadas.

7.7 Disponibilidad de indicadores para la navegación en línea fundamentada

El Código reforzado no tiene como objetivo evaluar la veracidad de los contenidos editoriales. No obstante, dada la abundancia de información disponible en línea, los usuarios afrontan desafíos sobre qué fuentes de información se pueden consultar y en cuáles se puede confiar. Los indicadores de fiabilidad, centrados en la integridad de la fuente y desarrollados por terceras partes independientes, en colaboración con los medios informativos, incluidas asociaciones de periodistas y organizaciones en favor de la libertad de los medios de comunicación, así como verificadores de datos, pueden ayudar a los usuarios a tomar decisiones fundamentadas[62].

Los signatarios pueden facilitar el acceso a estos indicadores ofreciendo a los usuarios la posibilidad de usarlos en sus servicios. En ese caso, el Código reforzado debe garantizar que los signatarios aporten transparencia respecto a dichos indicadores de terceras partes, también en lo relativo a su metodología.

---

[61] Las optimizaciones pueden estar relacionadas, por ejemplo, con el diseño virtual, el momento o la presentación gráfica de la intervención.

[62] Algunos ejemplos de estos indicadores pueden ser el Global Disinformation Index, la Journalism Trust Initiative o el Trust Project, así como el servicio NewsGuard.

La aplicación de estos indicadores de fiabilidad debe estar en total consonancia con los principios de libertad de prensa y pluralismo. Para tal fin, debe corresponder a los usuarios decidir si quieren usar esas herramientas[63].

7.8 Medidas para frenar la desinformación en aplicaciones de mensajería

Además de las últimas iniciativas desarrolladas en cooperación con los verificadores de datos[64], los signatarios que ofrezcan aplicaciones de mensajería privada deben poner a prueba y aplicar características técnicas que ayuden a los usuarios a identificar la desinformación difundida a través de dichos servicios. Estas soluciones deben ser compatibles con la naturaleza de estos servicios y, en particular, con el derecho a las comunicaciones privadas, sin un debilitamiento del cifrado. Estas características pueden, por ejemplo, ayudar a los usuarios a verificar si contenidos concretos que reciben han sido verificados como falsos. Esto puede lograrse, por ejemplo, a través de soluciones que hagan visibles las etiquetas de verificación de datos cuando el contenido de los medios sociales se difunda en una aplicación de mensajería. Asimismo, los signatarios deben considerar soluciones que permitan a los usuarios comprobar los contenidos que reciben en una aplicación de mensajería usando un repositorio de verificaciones de datos.

8 EMPODERAMIENTO DE LA COMUNIDAD INVESTIGADORA Y DE VERIFICACIÓN DE DATOS

En vistas de su contribución esencial en favor de una estrategia eficaz destinada a abordar la desinformación, el Código reforzado debe establecer un marco para el acceso sólido a los datos de las plataformas por parte de la comunidad investigadora y de verificación de datos, así como un apoyo adecuado para sus actividades.

8.1 Acceso a los datos de los signatarios para la investigación sobre la desinformación

Al ofrecer análisis basados en datos, los investigadores resultan esenciales para lograr un adecuado entendimiento de la evolución de los riesgos vinculados a la desinformación[65], y pueden ayudar a desarrollar mecanismos de reducción de riesgos. Esta labor depende esencialmente del acceso a los datos de las plataformas. La propuesta de Ley de servicios digitales ofrece un mecanismo regulador para que los investigadores autorizados puedan acceder a los datos para investigar los riesgos derivados de los servicios de las plataformas[66]. El Código reforzado debe crear un marco que, ya en el período intermedio antes de la adopción de la Ley de servicios digitales, ofrezca a los investigadores el acceso necesario a los datos de las plataformas y que igualmente facilite a largo plazo el

[63] Las herramientas para evaluar la fiabilidad de las fuentes de información, como las llamadas marcas de confianza, deben facilitarse a los usuarios para que estos las consulten si lo desean. También se puede dar a los usuarios la opción de contar con señales relacionadas con la fiabilidad de las fuentes periodísticas incluidas en los sistemas automatizados que seleccionan y clasifican el contenido que aparece en sus canales de usuario.

[64] Las organizaciones de verificación de datos, apoyadas por algunos proveedores de aplicaciones de mensajería, ofrecen a los usuarios de estas aplicaciones la posibilidad de verificar los datos de los mensajes que reciben a través de esos canales privados: https://faq.whatsapp.com/general/ifcn-fact-checking-organizations-on-whatsapp/?lang=es.

[65] Asimismo, esto resulta esencial para informar a los signatarios, la Comisión, las autoridades nacionales competentes y el público.

[66] El artículo 31 en particular.

desarrollo de un marco específico para un acceso a los datos adaptado para llevar a cabo actividades de investigación sobre el fenómeno de la desinformación.

8.1.1 Marco general para el acceso a los datos

Para el Código reforzado, los signatarios correspondientes, en particular las plataformas, deben comprometerse a crear conjuntamente un marco sólido para el acceso a los datos para fines de investigación. Las condiciones para el acceso deben ser transparentes, abiertas y no discriminatorias, proporcionadas y justificadas. En el caso de los datos personales, las condiciones deben cumplir el RGPD. En general, las condiciones de acceso a cualquier dato deben respetar el derecho a las comunicaciones privadas y proteger de forma adecuada los derechos e intereses legítimos de todas las partes afectadas.

Los signatarios deben desarrollar el marco en cooperación con la comunidad investigadora, el EDMO y las autoridades nacionales pertinentes. Los compromisos deben incluir un calendario detallado del progreso previsto en el diseño y aplicación del marco.

Este debe contemplar diferentes accesos a los sistemas de datos con salvaguardias adecuadas para i) los datos anonimizados y no personales y ii) los datos que exigen un control adicional, incluidos los datos personales. El marco debe ofrecer la posibilidad de acceder en tiempo real a ciertos tipos de datos, a fin de permitir la rápida evaluación de los riesgos emergentes y en evolución, así como el diseño de medidas de reducción adecuadas.

Aunque el marco está en desarrollo, los signatarios deben poner a prueba soluciones temporales. Por ejemplo, el uso de espacios controlados puede ofrecer a un número limitado de investigadores acceso a datos pertinentes de las plataformas para investigar temas específicos que sirvan de base para el diseño del marco y de soluciones operativas de prueba para un mayor acceso a los datos en las plataformas.

8.1.2 Acceso a datos anonimizados y no personales

El Código reforzado debe incluir un compromiso para ofrecer, siempre que sea viable, un acceso continuo, en tiempo real, estable y armonizado a datos anonimizados, agregados o, de lo contrario, no personales para fines de investigación a través de API u otras soluciones técnicas abiertas y accesibles que permitan la explotación óptima de los conjuntos de datos.

El acceso a soluciones de datos debe facilitar la búsqueda y análisis de estos. Los signatarios correspondientes deben garantizar que las funcionalidades de los sistemas de acceso satisfacen las necesidades de los investigadores y son interoperables. Los compromisos deben garantizar procedimientos para informar sobre el mal funcionamiento de los sistemas de acceso, así como la restauración de este y la reparación de las funcionalidades defectuosas en un tiempo razonable.

8.1.3 Acceso a datos que exigen un control adicional, incluidos los datos personales

Los datos que pueden exponer información personal, incluida información sensible[67], exigen un control y salvaguardias adicionales. La información confidencial, en particular los secretos comerciales, o los datos vinculados a la seguridad de los servicios de las plataformas también merecen una protección adecuada. Al mismo tiempo, el marco para el acceso a los datos debe permitir al menos a los investigadores del mundo académico acceder a los conjuntos de datos necesarios para entender las fuentes, vectores, métodos y patrones de propagación que caracterizan al fenómeno de la desinformación.

Para tal fin, el Código debe crear un procedimiento transparente que implique a todas las partes interesadas pertinentes, en particular, las plataformas y la comunidad investigadora, para definir las condiciones aplicables para el acceso a estos conjuntos de datos. En principio, las condiciones deben estar normalizadas y ser uniformes en todas las plataformas. El procedimiento debe regular, entre otras cosas, i) las normas y la cualificación mínimas para los investigadores a los que se conceda el acceso, ii) las categorías de datos mínimas que se facilitarán, iii) las medidas de seguridad técnicas y organizativas que deben respetarse en el tratamiento de dichos datos, incluida la limitación de la finalidad y la minimización de datos y iv) respecto a los datos seudonimizados, todas las medidas necesarias para impedir la reasignación[68].

8.1.4 Función del EDMO

En vistas de su independencia y de sus funciones de coordinación, el EDMO puede ofrecer apoyo en el ámbito del acceso a los datos, incluido a través de orientaciones, entre otras cosas, sobre las categorías de datos que deben facilitarse, las finalidades para las que puede efectuarse el tratamiento de datos y las medidas de seguridad adecuadas para tratar datos personales y evitar la reasignación de datos anonimizados.

Con la ayuda del EDMO, se están llevando a cabo labores para explorar las posibilidades de un código de conducta en virtud del artículo 40 del RGPD destinado a garantizar una aplicación adecuada de los requisitos de protección de los datos y de la intimidad para el intercambio de datos personales por parte de las plataformas con los investigadores. El RGPD ofrece unas condiciones generales de tratamiento de datos personales también en forma de intercambio de datos personales por parte de las plataformas con los investigadores. Un código así reduciría las inseguridades jurídicas y los riesgos para las plataformas que ofrecen acceso a los datos, y garantizaría un entorno seguro y armonizado para el tratamiento de datos personales para fines de investigación[69]. El Código reforzado debe comprometer a los signatarios a facilitar, en caso necesario, el desarrollo del código de conducta en virtud del artículo 40 del RGPD.

---

[67] En el sentido del artículo 9 del RGPD.

[68] Como exige el RGPD, cuando se trata de datos personales, su comunicación debe fundamentarse en una base jurídica clara con salvaguardias adecuadas, incluido el régimen del artículo 9 para las categorías especiales de datos.

[69] El debate de las partes interesadas mostró el apoyo de los signatarios del Código y la comunidad investigadora a esta iniciativa: https://digital-strategy.ec.europa.eu/en/library/summary-multi-stakeholder-discussions-preparation-guidance-strengthen-code-practice-disinformation.

8.1.5 Acceso a los datos para otras partes interesadas

Otras partes interesadas, como las organizaciones de la sociedad civil, los centros de investigación no académicos y los periodistas de investigación, también desempeñan papeles importantes en la detección y análisis de las campañas de desinformación, la elaboración de respuestas políticas, así como la promoción de la sensibilización pública y la resiliencia social. Los signatarios del Código deben facilitar, en particular a los Estados miembros en los que no haya una capacidad académica adecuada, un nivel de acceso suficiente a dichas partes interesadas que sea coherente con los requisitos de intimidad y que esté sujeto a un control reforzado contra el uso indebido de los datos personales y la reasignación de los datos seudonimizados.

8.2 Marco de cooperación entre los signatarios y los investigadores

Para fomentar una mayor comunidad multidisciplinar de investigadores independientes, y para empoderarla, el Código debe establecer un marco para una cooperación transparente, abierta y no discriminatoria entre los signatarios y la comunidad investigadora de la UE respecto a los recursos y el apoyo facilitados a los investigadores. Dicho marco debe permitir a la comunidad investigadora gestionar de forma independiente los fondos facilitados por los signatarios para la investigación sobre la desinformación, la definición de prioridades científicas y unos procedimientos de asignación transparentes basados en el mérito científico. En este sentido, el EDMO puede colaborar en la asignación de dichos recursos.

8.3 Colaboración con los verificadores de datos

Los verificadores de datos son agentes importantes a la hora de abordar el fenómeno de la desinformación[70]. Evalúan y verifican los contenidos a partir de datos, pruebas e información contextual, y conciencian a los usuarios acerca de la desinformación en línea. El Código reforzado debe prever un mayor apoyo a su labor y aumentar la cobertura de las actividades de verificación de datos en todos los Estados miembros y lenguas de la UE.

8.3.1 Formas de cooperación

En vista de las carencias significativas y la aplicación desigual de las actividades de verificación de datos en los servicios y los Estados miembros[71], los signatarios de las plataformas deben comprometerse a dar pasos concretos, con objetivos y plazos claros, para ampliar su cooperación con los verificadores de datos con el fin de garantizar la aplicación coherente de la verificación de datos en sus servicios. Los esfuerzos deben centrarse especialmente en los Estados miembros y las lenguas en los que aún no se ofrece la verificación de datos [72].

---

[70] Las organizaciones de verificación de datos publican periódicamente informes imparciales sobre la precisión de las afirmaciones realizadas por figuras públicas e instituciones importantes y sobre otras declaraciones de interés para la sociedad ampliamente divulgadas. Son independientes y siguen estrictas normas éticas y de transparencia, como las definidas por la Red Internacional de Verificación de Datos (IFCN) (https://www.poynter.org/international-fact-checking-network-fact-checkers-code-principles).

[71] https://www.disinfo.eu/publications/bulgaria%3A-the-wild-wild-east-of-vaccine-disinformation/.

[72] Mapa de actividades de verificación de datos del EDMO en la UE: https://edmo.eu/fact-checking-activities/.

Esto puede lograrse a través de acuerdos multilaterales entre las plataformas y las organizaciones independientes de verificación de datos que cumplan estrictas normas éticas y profesionales. Dichos acuerdos deben basarse en condiciones transparentes, abiertas y no discriminatorias, y garantizar la independencia de los verificadores de datos. Los acuerdos deben ofrecer una remuneración justa a los verificadores datos por el trabajo usado por las plataformas, fomentar la cooperación transfronteriza entre ellos y facilitar su circulación entre los servicios de los signatarios.

En vista de su función a la hora de fomentar actividades conjuntas de verificación de datos, el EDMO es idóneo para apoyar a las plataformas y los verificadores de datos a la hora de desarrollar un marco de colaboración, incluida la creación de una interfaz común para verificadores de datos, el intercambio de información entre estos y la promoción de la cooperación transfronteriza[73].

8.3.2 Uso e integración de la verificación de datos en los servicios de los signatarios

El Código reforzado debe incluir compromisos que exijan un uso e integración más coherentes de la labor de los verificadores de datos en los servicios de las plataformas, incluidos en los sistemas de publicidad programática y en los contenidos de vídeo. Las plataformas deben comprometerse a emplear mecanismos que permitan una incorporación inmediata y coherente de las verificaciones de datos a sus servicios tras la notificación de los verificadores, incluido un etiquetado rápido y eficiente. Los signatarios correspondientes deben facilitar la creación de un repositorio común de artículos sobre verificación de datos (verificaciones de datos) elaborados por verificadores y explorar las soluciones técnicas para facilitar su uso eficiente en todas las plataformas y lenguas para evitar el resurgimiento de la desinformación que ha sido desacreditada por los verificadores de datos[74].

8.3.3 Acceso de los verificadores de datos a información pertinente

Para maximizar la calidad y la repercusión de la verificación de datos, el Código reforzado debe garantizar que los signatarios de las plataformas se comprometan a ofrecer a los verificadores de datos acceso automatizado a la información sobre las medidas que han adoptado respecto a los contenidos verificados y las verificaciones de datos. La información debe cuantificar i) las interacciones de los usuarios a lo largo del tiempo (por ejemplo, número de visitas, clics en me gusta, clics en compartir o comentarios antes y después de la verificación de datos)[75] con los contenidos que han sido verificados, y ii) el alcance de las verificaciones de datos a lo largo del tiempo en los servicios en línea en los que se publicaron. Las plataformas y verificadores de datos deben acordar una interfaz común para la verificación de datos con el fin de garantizar la coherencia en la forma en la que las plataformas usan, atribuyen y ofrecen comentarios sobre la labor de los verificadores de datos. Además, el Código debe prever el

[73] Para seguir apoyando la labor de los verificadores de datos europeos, así como su cooperación y el desarrollo de nomas profesionales comúnmente acordadas, el proyecto piloto «Integridad de los medios sociales» ayudará a elaborar un código de integridad profesional para los verificadores de datos europeos en cooperación con el EDMO. Véase: programa anual de trabajo, adoptado en virtud de la Decisión C (2020) 2259 de la Comisión.

[74] Respecto a la creación de un repositorio de verificaciones de datos, los signatarios pueden buscar sinergias con el EDMO.

[75] Esto también debe incluir los datos demográficos y la localización anonimizados de las personas que comparten/reciben contenidos verificados.

intercambio periódico de información entre los signatarios correspondientes del mismo y la comunidad de verificación de datos con el fin de reforzar la cooperación.

9 SEGUIMIENTO DEL CÓDIGO

El Código reforzado debe complementarse con un sistema de seguimiento sólido, basado en la experiencia de la Comisión hasta la fecha en el seguimiento del Código, incluido el programa de la COVID-19. El sistema de seguimiento mejorado debe ofrecer una evaluación periódica de la aplicación por parte de los signatarios de los compromisos del Código, estimular mejoras en sus políticas y medidas, así como permitir la evaluación de la eficacia del Código como herramienta para abordar la desinformación. Asimismo, debe reforzar la rendición de cuentas de las plataformas en línea en el período intermedio antes de la adopción de la Ley de servicios digitales, y ofrecer un marco, entre otras cosas, para un diálogo estructurado con las plataformas de muy gran tamaño sobre el desarrollo e implantación de medidas de evaluación y mitigación del riesgo, en previsión de las obligaciones jurídicas previstas para ellas en la propuesta de Ley de servicios digitales.

En vista de estos objetivos, los actuales compromisos del Código sobre seguimiento deben reforzarse y ampliarse para crear un marco sólido que incorpore los elementos principales que se exponen más adelante. El Código reforzado debe garantizar en particular que los signatarios ofrezcan la información y los datos para el seguimiento en formatos normalizados, con desgloses por Estado miembro y de forma oportuna.

9.1 Indicadores clave de rendimiento

El seguimiento del Código debe basarse en indicadores clave de rendimiento capaces de medir la aplicación y eficacia de los compromisos del Código y la repercusión de este sobre el fenómeno de la desinformación. Para tal fin, existen dos clases de indicadores clave de rendimiento pertinentes: i) indicadores del nivel de servicio, que miden los resultados y la repercusión de las políticas aplicadas por los signatarios para cumplir sus compromisos en virtud del Código, y ii) indicadores estructurales, que miden la repercusión general del Código sobre la desinformación en la UE.

9.1.1 Indicadores del nivel de servicio

En virtud del Código revisado, los signatarios deben comprometerse a elaborar indicadores concretos del nivel de servicio. Los indicadores del nivel de servicio deben medir de forma eficaz la aplicación de los compromisos del Código y la repercusión de las políticas de los signatarios. Los indicadores deben ser suficientemente flexibles para atender a la distinta naturaleza de los servicios de los signatarios al tiempo que permiten realizar informes y comparaciones coherentes en todos los servicios.

El Código reforzado debe exigir a los signatarios que identifiquen (además de informar sobre él y comprometerse con él) un conjunto mínimo de indicadores cualitativos y cuantitativos destinados a evaluar, entre otras cosas:

- La repercusión de las herramientas y características aplicadas para mejorar la concienciación de los usuarios y su empoderamiento, incluidas las interacciones de estos con dichas herramientas y características[76].
- La repercusión de las herramientas y características que presentan o hacen más visible la información fiable de interés público, incluidas las interacciones de los usuarios con dichas herramientas y características[77].
- El número de verificaciones de datos, el porcentaje del contenido verificado frente al contenido señalado por los usuarios y la financiación aportada para actividades de verificación de datos.
- La repercusión de las actividades de verificación de datos y las interacciones de los usuarios con la información verificada como falsa o engañosa[78].
- El número de recursos en relación con las medidas adoptadas sobre el contenido por parte de las plataformas como resultado de señalar la desinformación y la información relativa a su resultado.
- El número de páginas, cuentas, perfiles y grupos que comparten desinformación y que están sometidos a medidas que reducen su visibilidad[79] y la cantidad de contenidos de este tipo compartido.
- La repercusión de los comportamientos manipuladores inadmisibles identificados, incluidos ejemplos de contenidos o cuentas eliminados o relegados[80].
- El número de relaciones entre los signatarios del Código procedentes del sector publicitario y entidades terceras encargadas de evaluar la calidad de las fuentes de información.
- La repercusión de las medidas empleadas para el control de la colocación de anuncios[81].
- La cantidad y el nivel de detalle de los datos facilitados para fines de investigación y el número de organizaciones de investigación europeas que tienen acceso a los datos de las plataformas.
- La cantidad de recursos facilitados por los signatarios para la investigación sobre la desinformación y el número de organizaciones de investigación europea que tienen acceso a dichos recursos.

---

[76] La repercusión puede medirse a través de indicadores que cuantifiquen el nivel de interacción (por ejemplo, visitas, frecuencias de clics, clics en compartir, etc.) de los usuarios con dichas herramientas y calificando la percepción de los usuarios respecto a la utilidad de estas. Asimismo, los indicadores deben incluir datos sobre el uso de las herramientas para señalar contenidos percibidos como falsos, e informar acerca de ellos.

[77] La repercusión puede medirse a través de indicadores que cuantifiquen el nivel de interacción (por ejemplo, visitas, impresiones, frecuencias de clics, clics en compartir, etc.) de los usuarios que dichas herramientas y calificando la percepción de los usuarios respecto a la utilidad de estas.

[78] La repercusión puede medirse a través de indicadores que cuantifiquen el nivel de interacción (por ejemplo, visitas, frecuencias de clics, clics en compartir, etc.) con fragmentos de contenido antes y después de ser etiquetados o relegados por haber sido verificados como falsos. Otros indicadores también pueden aportar información sobre cómo se producen las interacciones de los usuarios.

[79] Incluidas medidas como bajar la clasificación de contenidos, así como cerrar perfiles y grupos.

[80] La repercusión puede medirse a través de indicadores que cuantifiquen el nivel de interacción (por ejemplo, visitas, frecuencias de clics, clics en compartir, etc.) con contenidos, cuentas y ejemplos antes de ser eliminados y antes o después de ser relegados.

[81] La repercusión puede medirse a través de indicadores que cuantifiquen el número de colocaciones de anuncios presentadas en sitios web que provean constantemente contenidos de desinformación y el número de anuncios con contenidos de desinformación que hayan sido eliminados.

- La información relativa a la mano de obra humana implicada en el cumplimiento de los compromisos del Código[82].

9.1.2 Indicadores estructurales

Los signatarios del Código también deben comprometerse a contribuir al desarrollo de indicadores estructurales que puedan medir de forma eficaz la repercusión general del Código en el fenómeno de la desinformación. Como se describe más adelante, los signatarios deben crear un grupo de trabajo permanente cuyas tareas incluirán el desarrollo, puesta a prueba y ajuste de indicadores estructurales.

Estos pueden, por ejemplo, basarse en muestras representativas de usuarios de varios Estados miembros con el objetivo de medir la prevalencia de proveedores constantes de desinformación[83] en el consumo de medios de comunicación en línea de los ciudadanos europeos[84]. Dichos indicadores pueden medir el compromiso público con las fuentes de información, así como las encuestas periódicas y normalizadas para medir la exposición de los ciudadanos a la desinformación.

Hasta que se desarrolle un conjunto más estable de indicadores estructurales, los signatarios y las partes interesadas deben acordar un conjunto mínimo viable de indicadores estructurales que puedan aplicarse y ponerse a prueba rápidamente, trabajando para desarrollar un conjunto estable de indicadores estructurales eficaces.

9.2 Marco de seguimiento

El marco de seguimiento debe permitir la evaluación periódica de la aplicación por parte de los signatarios de los compromisos del Código, incluidos los cambios y evoluciones de las políticas y medidas pertinentes. Para tal fin, los signatarios deben informar periódicamente a la Comisión acerca de la aplicación de sus compromisos, incluidos los indicadores clave de rendimiento pertinentes.

Tras la experiencia positiva de los programas de seguimiento durante las elecciones de la UE de 2019[85] y la pandemia de COVID-19, la Comisión contará con el apoyo del Grupo de Entidades Reguladoras Europeas para los Servicios de Comunicación Audiovisual (ERGA) para el seguimiento de la aplicación del Código en los Estados miembros. El EDMO y sus centros también ayudan a la Comisión a analizar la información y los datos notificados por los signatarios y a evaluar la repercusión del Código a nivel nacional y de la UE.

Teniendo en cuenta el asesoramiento experto y el apoyo del ERGA y el EDMO, la Comisión evaluará periódicamente los avances realizados en la aplicación del Código, así como la repercusión del mismo en el fenómeno de la desinformación, y publicará sus

---

[82] Esta incluye el número de trabajadores empleados para llevar a cabo actividades destinadas a luchar contra la desinformación y las lenguas cubiertas por sus actividades.
[83] La identificación de proveedores en línea de desinformación debe basarse en una metodología clara y acordada definida por un amplio grupo de partes interesadas, incluidos investigadores académicos, verificadores de datos, ONG y organizaciones de la sociedad civil.
[84] El mecanismo de medición para los indicadores estructurales puede inspirarse en la labor realizada por el sector audiovisual para medir audiencias.
[85] https://erga-online.eu/wp-content/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf.

conclusiones. Asimismo, la Comisión ofrecerá nuevas orientaciones sobre cómo deben abordar los signatarios las restantes carencias y deficiencias del Código.

9.2.1 Informes periódicos

Las obligaciones de presentación de informes en virtud del Código reforzado deben tener en cuenta el tamaño de los signatarios y el tipo de servicios que ofrecen. Los proveedores de servicios en línea ampliamente usados en la UE y con unos elevados perfiles de riesgo respecto a la propagación de la desinformación deben informar cada seis meses acerca de la aplicación de los compromisos que han suscrito y deben ofrecer los correspondientes indicadores del nivel de servicio. Asimismo, deben evaluar anualmente los riesgos vinculados al fenómeno de la desinformación. Otros signatarios del Código deben informar anualmente y ofrecer datos correspondientes a sus actividades. Los signatarios que ofrezcan herramientas, instrumentos o soluciones para luchar contra la desinformación, o que apoyen al Código ofreciendo su experiencia, también deben informar anualmente sobre sus actividades y conclusiones pertinentes para la aplicación y eficacia del Código. La presentación de informes debe realizarse de conformidad con un calendario definido que establezca los períodos de cobertura y los plazos de presentación. Los datos usados para medir los indicadores clave de rendimiento deben incluir desgloses por Estado miembro.

La presentación de informes debe basarse en un modelo normalizado que permita realizar, en la medida de lo posible, comparaciones entre las plataformas. Además, los signatarios deben acordar una serie de formatos normalizados y auditables para aportar datos relacionados con los indicadores clave de rendimiento. Estos formatos deben desarrollarse de forma conjunta con las partes interesadas pertinentes del grupo de trabajo permanente, y deben cumplir las normas y utilizar métodos de la comunidad investigadora y de verificación de datos. Finalmente, estos formatos deben permitir la actualización continua de un cuadro de indicadores público facilitado a través del centro de transparencia, como se describe a continuación.

9.2.2 Centro de transparencia

Para mejorar la transparencia y la rendición de cuentas en torno a la aplicación del Código, los signatarios deben comprometerse a crear y mantener un centro de transparencia de acceso público. Los signatarios deben indicar en dicho centro las políticas específicas que han adoptado para aplicar cada compromiso del Código que hayan suscrito, y ofrecer información básica sobre cómo se cumplen dichas políticas, como son la cobertura geográfica y lingüística. Asimismo, debe contar con un cuadro de indicadores que presente los indicadores clave de rendimiento pertinentes. El centro de transparencia debe diseñarse, en particular, con vistas a permitir realizar comparaciones entre servicios de los avances de los signatarios en la aplicación de los compromisos del Código y a lograr una repercusión cuantificable en la lucha contra la desinformación. Los signatarios deben comprometerse a mantener el centro de transparencia periódicamente actualizado y a divulgar cualquier cambio de las políticas pertinentes no más tarde de treinta días después de que se anuncie o aplique un cambio.

9.2.3 Grupo de trabajo permanente

El Código reforzado debe crear un grupo de trabajo permanente cuyo objetivo sea desarrollar y adaptar el Código teniendo en cuenta los avances tecnológicos, sociales, legislativos y del mercado. El grupo de trabajo debe incluir a signatarios del Código y representantes del EDMO y el ERGA, y puede invitar a expertos pertinentes para que apoyen su labor. El grupo de trabajo debe estar presidido por la Comisión e incluir

representantes del Servicio Europeo de Acción Exterior. De conformidad con el objetivo general de ofrecer aportaciones para la revisión y adaptación del Código, las actividades del grupo de trabajo deben incluir, entre otras cosas:

- Establecer una metodología de evaluación del riesgo y un sistema de respuesta rápida que se debe usarse en situaciones especiales, como las elecciones o las crisis.
- Revisar la calidad y eficacia del modelo de notificación armonizado, así como los formatos y métodos de divulgación de datos para fines de seguimiento.
- Optimizar la calidad y la precisión de los datos que deben aportarse para la medición de los indicadores.
- Contribuir a la evaluación de la calidad y la eficacia de los indicadores del nivel de servicio y su adaptación pertinente.
- Desarrollar, poner a prueba y ajustar los indicadores estructurales y diseñar mecanismos para medirlos en los Estados miembros.
- Ofrecer aportaciones expertas y datos actualizados pertinentes para los compromisos del Código como, por ejemplo, nuevas formas de comportamientos dolosos.

10 CONCLUSIONES Y PRÓXIMAS ETAPAS

Las Orientaciones establecen elementos esenciales necesarios, desde el punto de vista de la Comisión, para transformar el Código en un instrumento más sólido para abordar la desinformación y crear un entorno en línea más seguro y transparente.

La Comisión insta a los signatarios del Código a reunirse y reforzar el Código, de conformidad con las presentes Orientaciones. La Comisión invita a los signatarios a ofrecer un primer borrador del Código revisado en otoño para facilitar un debate adecuado. Asimismo, invita a los posibles nuevos signatarios a que se unan al Código y participen en su revisión, como son las plataformas establecidas y emergentes, los agentes empresariales y otros participantes del sector de la publicidad en línea, así como otras partes interesadas que pueden contribuir con sus recursos o experiencia al funcionamiento eficaz del Código.

Dado que la desinformación es un fenómeno que no tiene fronteras y con el fin de reforzar la repercusión real del Código de Buenas Prácticas, las medidas adoptadas en la vecindad europea resultarán útiles, como el trabajo con la sociedad civil, la cooperación con los profesionales de los medios de comunicación y las iniciativas en materia de alfabetización mediática.