4 Actualizar las medidas de gobernanza y la arquitectura institucional para reforzar la integridad del espacio informativo

Este capítulo analiza cómo los países están actualizando sus medidas de gobernanza y su arquitectura institucional para fortalecer la integridad del espacio informativo. Estudia la función que desempeñan los marcos estratégicos y los mecanismos de coordinación intergubernamental para lograr un enfoque coherente en la elaboración de políticas públicas. También, analiza la necesidad de equipar a los funcionarios públicos con las competencias y los recursos necesarios para tener una mejor comprensión de los riesgos planteados por la desinformación. Por último, explora el papel de una gobernanza reglamentaria adaptada, que favorezca un entorno en el que pueda prosperar la información fiable y de calidad.

Este capítulo incluye datos de 24 países miembros de la OCDE obtenidos de la encuesta «Arquitectura institucional y prácticas de gobernanza para fortalecer la integridad de la información», diseñada por el equipo del Centro de Recursos DIS/MIS de la OCDE. Los países que han respondido a esta encuesta son: Australia, Canadá, Chile, Colombia, Costa Rica, Estonia, Finlandia, Francia, Alemania, Grecia, Italia, Irlanda, Letonia, Lituania, Luxemburgo, Países Bajos, Noruega, Portugal, República Eslovaca, España, Suecia, Suiza, Turquía y Estados Unidos.

4.1. INTRODUCCIÓN

Los gobiernos de la OCDE están adaptando sus instituciones y medidas políticas para responder a las amenazas que plantea la desinformación y crear un entorno favorable para que prospere la información precisa, fiable y plural. Desde el punto de vista de la gobernanza, el reto es significativo, ya que los gobiernos se hallan en una posición compleja: se necesitan medidas para contrarrestar la desinformación y reforzar la integridad de la información. Sin embargo, dichas medidas no deben en ningún caso y bajo ninguna circunstancia llevar a un mayor control de la información ni socavar la libertad de expresión.

La variedad de amenazas que plantean las campañas de desinformación, desde las teorías conspirativas sobre salud pública hasta la manipulación informativa y la injerencia por parte de agentes extranjeros, tal como se vio recientemente durante la pandemia de COVID-19 y la manipulación de la información por parte de Rusia para socavar el (European Union External Action Service, 2023[1]) apoyo internacional a Ucrania, han actuado como un catalizador para que los gobiernos aborden este fenómeno global de manera coordinada.

Para lograrlo, es fundamental establecer marcos estratégicos a nivel nacional, unidades de coordinación administrativa y grupos de trabajo especializados. Además, se necesita invertir en el desarrollo de capacidades en las administraciones públicas para elaborar políticas respaldadas por evidencia y adaptadas al problema que se pretende resolver. En este sentido, los gobiernos deben evaluar sus medidas políticas y prácticas institucionales para fortalecer la integridad del espacio informativo, reconociendo que:

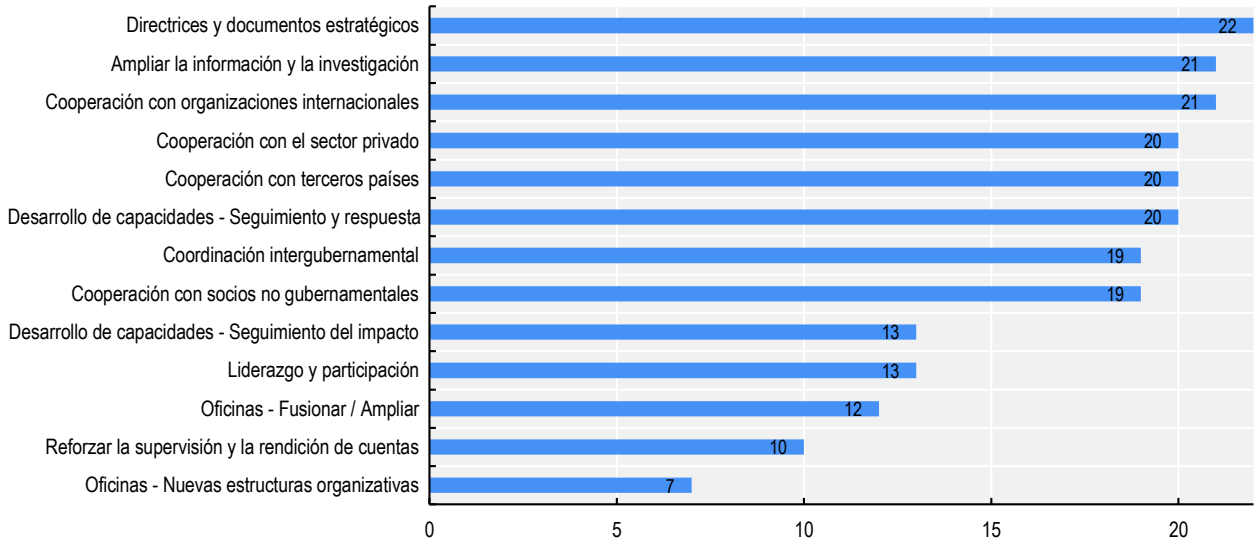
- Se necesita orientación estratégica y esfuerzos coordinados, a nivel nacional e internacional.
- Un espacio de la información en constante evolución requiere que los gobiernos inviertan en programas de formación y de infraestructura tecnológica dentro de las administraciones públicas, para poder desarrollar unas políticas coherentes e integrales.
- Los gobiernos deben adaptar y actualizar una gobernanza regulatoria que impulse un entorno propicio para que prospere la información fiable.

4.2. LA COORDINACIÓN GUBERNAMENTAL Y LA ORIENTACIÓN ESTRATÉGICA SON ESENCIALES PARA HACER FRENTE A LA DESINFORMACIÓN

Un fenómeno multifacético y complejo como la desinformación, que implica múltiples actores, canales y tácticas, requiere un enfoque coordinado y estratégico en materia de políticas públicas. La rápida proliferación de contenidos falsos y engañosos ha concienciado a los países de la necesidad de desarrollar una visión integral sobre cómo mejorar el grado de integridad en el espacio informativo. Para ello, los gobiernos están creando o actualizando gradualmente sus mecanismos de coordinación. Dentro de los países, los mecanismos de coordinación varían mucho y pueden consistir en oficinas centrales (ya sean unidades, células, etc.) o grupos de trabajo interinstitucionales conformados por funcionarios públicos. Estos últimos suelen tener mandatos y áreas de actuación específicos.

La prioridad dada a los aspectos de coordinación es clara: casi todos los participantes de la encuesta de la OCDE identificaron el desarrollo, la actualización o el incremento de la relevancia de los documentos de políticas y/o estrategias nacionales como una prioridad principal[1] (Figura 4.1). La mayoría de los países encuestados también señalaron la importancia de una mejor coordinación dentro y fuera del gobierno, así como el desarrollo de capacidades para identificar y responder a las amenazas de la desinformación. Estas prioridades proporcionan un marco para orientar las prioridades de los gobiernos hacia el objetivo de fortalecer la integridad de la información.

Figura 4.1. Áreas que mejorar en el futuro para reforzar la integridad de la información



Nota: núm.= 22
Fuente: Encuesta de la OCDE sobre arquitectura institucional y prácticas de gobernanza para fortalecer la integridad de la información, 2023.

4.2.1. Elaborar marcos estratégicos para combatir la desinformación y reforzar la integridad de la información es una prioridad

Los marcos estratégicos son esenciales para establecer una visión coherente y una respuesta eficaz en el fortalecimiento de la integridad del espacio informativo. Las estrategias nacionales pueden proporcionar claridad al permitir establecer responsabilidades institucionales, prevenir la duplicación de esfuerzos y contribuir a evitar asimetrías de información en la administración pública. Es importante recalcar que un documento estratégico no es un fin en sí mismo, sino un medio para guiar el diseño de medidas políticas y establecer plazos de evaluación para determinar el correcto funcionamiento y el progreso de las políticas implementadas (OECD, 2020[2]).

Algunos países, especialmente en los últimos años, han desarrollado estrategias nacionales centradas específicamente en luchar contra la desinformación y reforzar la integridad de la información. Sin embargo, los datos de la encuesta de la OCDE muestran que solo nueve países (Australia, Estonia, Letonia, Lituania, Portugal, España, Países Bajos, Italia y Estados Unidos) han desarrollado un documento estratégico, que proporciona orientación sobre cómo combatir la desinformación y reforzar la integridad de la información a nivel nacional.[2] Otros países, como Irlanda y Alemania, aún están en proceso de desarrollar estrategias nacionales específicamente centradas en estos temas.

Las estrategias de los países suelen abarcar aspectos operativos como la designación de puntos focales, la delimitación de competencias de los mecanismos de coordinación y el establecimiento de plazos para garantizar la implementación y la evaluación de las medidas políticas (véase un Recuadro 4.1 resumen de la estrategia nacional de los Países Bajos).

Recuadro 4.1. La estrategia del gobierno neerlandés para combatir la desinformación

En diciembre de 2022, los Ministerios neerlandeses de Asuntos de Interior y Relaciones con el Reino, Justicia y Seguridad, y Educación, Cultura y Ciencia presentaron ante la Cámara de Representantes una nueva estrategia gubernamental para proteger el debate público libre y abierto frente a la desinformación.

En el documento, presentan su estrategia nacional como un enfoque eficaz para abordar la información errónea y la desinformación centrado en los valores y los derechos fundamentales del estado de derecho, como la libertad de expresión y la libertad de prensa. Un punto importante de la estrategia de los Países Bajos es su afirmación de que la calificación de la desinformación como tal y la realización de verificaciones de hechos no constituyen un deber principal del gobierno. Sin embargo, el documento sí señala que cuando están en juego la seguridad nacional, la salud pública o la estabilidad social y/o económica, el gobierno puede actuar y desmentir la información falsa y engañosa.

La estrategia describe que el Ministro de Asuntos de Interior y Relaciones con el Reino tiene la responsabilidad de coordinar la política contra la desinformación y que actúa como el principal punto de contacto dentro del gobierno nacional y con las autoridades municipales y provinciales. El ministerio deberá desempeñar esta función promoviendo la colaboración entre las autoridades en este ámbito y cumpliendo una función de conocimiento. La estrategia también subraya la necesidad de contar con mecanismos de coordinación internacional, del Sistema Europeo de Alerta Temprana, del Centro Europeo de Excelencia para la Lucha contras las Amenazas Híbridas, el Centro de Excelencia StratCom de la OTAN y foros internacionales como la Unión Europea, el G7 y la OCDE. Esta estrategia actualiza la primera política gubernamental sobre desinformación presentada en 2019 (Documentos Parlamentarios II 2019/2020, 30821, núm. 91).

Fuente: Gobierno de los Países Bajos (2022[3]), *Government-wide strategy for effectively tackling disinformation*, https://www.government.nl/documents/parliamentary-documents/2022/12/23/government-wide-strategy-for-effectively-tackling-disinformation.

Además de las estrategias nacionales, en muchos países las orientaciones estratégicas para responder a la desinformación se incluyen como parte de otros documentos nacionales. Esto se debe en parte a la naturaleza multifacética de este fenómeno. Este es el caso de Australia, Colombia, Costa Rica, Estonia, Francia, Finlandia, Alemania, Luxemburgo[3] y República Eslovaca.

En Alemania y Estonia, por ejemplo, las medidas para combatir la desinformación vienen descritas en su política de seguridad nacional. La Estrategia de Seguridad Nacional alemana, adoptada por el Consejo de Ministros en junio de 2023, menciona diversas medidas para prevenir campañas de desinformación y comprender cómo se cruzan con otras amenazas a la seguridad nacional. En Estonia, el Concepto de Seguridad Nacional (actualizado en febrero de 2023) estipula un curso de acción para combatir la desinformación. En Australia, las políticas para combatir la desinformación también forman parte de sus prioridades en materia de interferencia digital y extranjera, a las que se hace referencia tanto en la Estrategia Internacional de Compromiso Cibernético y Tecnológico Crítico de Australia, como en la Estrategia Australiana de Lucha contra las Injerencias Extranjeras. En Francia, la Revisión Nacional Estratégica (*Revue nationale stratégique*, en francés), presentada por el presidente francés en octubre de 2022, ofrece una visión general del entorno de defensa y seguridad nacional e internacional del país, destacando la lucha contra la desinformación como una prioridad. La Revisión también ha sido el punto de partida de la Estrategia Nacional de Influencia, actualmente en proceso de elaboración por el Ministerio para Europa y de Asuntos Exteriores, y de la creación de unidades específicas para la lucha contra la desinformación en el seno de varios ministerios, incluido el Ministerio para Europa y Asuntos Exteriores y el Ministerio de Defensa.

Además, la República Eslovaca adoptó su Concepto de Comunicación Estratégica en junio de 2023, para servir de ayuda a la función de comunicación estratégica para

responder y mitigar los efectos nocivos de las operaciones de influencia en el espacio de la información y aumentar la confianza de los ciudadanos en las instituciones democráticas. Este documento detalla los esfuerzos para mejorar la comunicación entre el Estado y los ciudadanos, formalizar y agilizar la cooperación y coordinación de las instituciones públicas en la comunicación estratégica y acelerar la respuesta del Estado en la lucha contra la desinformación (Government of the Slovak Republic, 2023[4]).

Más allá del marco estratégico en sí, el proceso de desarrollo, implementación y posterior seguimiento de una estrategia exige atención. De hecho, un proceso de desarrollo de estrategias inclusivo y riguroso podría contribuir a garantizar que los objetivos promuevan metas democráticas y sean significativos para los ciudadanos (OECD, 2020[2]). Para garantizarlo, algunos países han creado grupos de trabajo que ayudan a articular este proceso. Por ejemplo, el Grupo de Trabajo Nacional de Estrategia contra la Desinformación, de Irlanda, creado en el 2023, fue el resultado de una recomendación de la Comisión irlandesa sobre el Futuro de los Medios de Comunicación (FoMC), que pedía un enfoque más coordinado y estratégico para combatir el impacto perjudicial de la desinformación en la sociedad y la democracia irlandesas (Recuadro 4.2).

Recuadro 4.2. Grupo de Trabajo sobre la Estrategia Nacional de Lucha contra la Desinformación de Irlanda

En 2022, el gobierno irlandés creó el «Grupo de Trabajo sobre la Estrategia Nacional de Lucha contra la Desinformación», coordinado por el Departamento de Turismo, Cultura, Artes, Gaeltacht, Deportes y Medios de Comunicación. El organismo incluye a representantes de la industria, del mundo académico, de la sociedad civil y de los departamentos gubernamentales.

Según lo recomendado por la Comisión irlandesa sobre el Futuro de los Medios de Comunicación, este grupo de trabajo es el encargado de desarrollar una Estrategia Nacional contra la Desinformación en consulta con todos los departamentos y organismos pertinentes, incluido el centro irlandés del Observatorio Europeo de los Medios Digitales, las partes interesadas de la industria, los medios de comunicación, los grupos de la sociedad civil, los verificadores de datos irlandeses y los investigadores de la desinformación. Para ello, se establecieron tres subgrupos encargados de examinar las áreas temáticas relativas a la desinformación, que abarcan:

- El mapeo de las iniciativas existentes;
- El examen del entorno normativo actual y emergente;
- El apoyo al periodismo libre, independiente y de alta calidad, y la protección de la información de interés público.

Cada subgrupo publicó un informe sobre su área temática. El período de consulta, ya finalizado, ha consistido en una consulta pública por escrito y un foro de consultas abierto a una amplia gama de partes interesadas. Está previsto que la Estrategia se publique a finales del primer trimestre de 2024.

La Estrategia tiene como objetivo coordinar los esfuerzos nacionales para combatir la desinformación y proporcionar un enfoque conjunto para garantizar que se apliquen restricciones efectivas a la creación y difusión de este material dañino. El grupo de trabajo también se encarga de desarrollar un seguimiento eficaz a largo plazo de la aplicación del Código de buenas prácticas en materia de desinformación y el Reglamento de servicios digitales en Irlanda. Las actas de las reuniones del grupo de trabajo y otros documentos relevantes se publican en el sitio web oficial del gobierno.

Fuente: Gobierno de Irlanda (2023[5]), National Counter Disinformation Strategy Working Group, https://www.gov.ie/en/publication/04f9e-national-counter-disinformation-strategy-working-group.

A medida que los esfuerzos del gobierno para construir la integridad de la información continúen desarrollándose, valdrá la pena avanzar en la comprensión de las tendencias y prioridades con el fin de aclarar y fortalecer el papel de la orientación estratégica en este ámbito.

4.2.2. Los mecanismos de coordinación gubernamentales deben tener objetivos, competencias y ámbitos de actuación claramente definidos

Un enfoque multiinstitucional coherente podría ayudar a los países a identificar sinergias entre las prioridades sectoriales, asignar unas responsabilidades claras, evitar la duplicación de esfuerzos y promover acciones de apoyo mutuo entre las instituciones que luchan contra la desinformación. Por ejemplo, establecer la capacidad operativa para rastrear, prevenir y desacreditar las campañas de manipulación de la información, a menudo requiere una coordinación a nivel estratégico para implementar sistemas, procesos y funciones de seguimiento, así como a nivel táctico, para garantizar que se puedan adoptar las medidas oportunas.

Las formas en que los países coordinan sus respuestas a las amenazas de la desinformación y los esfuerzos para mejorar la integridad de la información son muy variadas y evolucionan rápidamente. A nivel nacional, las responsabilidades se reparten por todo el sector público, incluido el gobierno, los ministerios competentes (incluidos seguridad, digital, comunicación, medios de comunicación, cultura, educación e investigación), las agencias de seguridad e inteligencia y los reguladores. La complejidad de los esfuerzos para reforzar la integridad de la información en las democracias exige el establecimiento de mecanismos de coordinación para facilitar la cooperación dentro y entre los gobiernos.

Los datos de la encuesta de la OCDE muestran que la mitad de los países encuestados (54 %) tienen por lo menos un mecanismo intergubernamental dedicado a coordinar los esfuerzos nacionales para identificar y responder a la desinformación y/o proporcionar asesoramiento técnico sobre políticas relacionadas con este asunto.[4] Estos mecanismos suelen funcionar como unidades centrales (como oficinas o células) con un mandato oficial para coordinar responsabilidades y/o como grupos de trabajo especializados, compuestos por funcionarios públicos de todo el gobierno (Figura 4.2).

Figura 4.2. Mecanismos de coordinación gubernamentales para combatir la desinformación

Unidad de coordinación intergubernamental

Unidad, oficina o célula gubernamental encargada de la coordinación de políticas y acciones entre diferentes organismos y/o niveles administrativos, para hacer frente a las amenazas que plantea la desinformación y mejorar la integridad de la información.

Las responsabilidades de coordinación pueden incluir el intercambio regular de información, el establecimiento de prioridades políticas y la implementación de un marco estratégico integrado de todo el gobierno.

Estos mecanismos de coordinación facilitan la asignación de recursos humanos y financieros, y evitan la duplicación de esfuerzos políticos, garantizando la colaboración vertical (autoridad central) y horizontal (coherencia interna y eficiencia) entre los organismos gubernamentales.

Los ejemplos incluyen:
- VIGINUM de Francia
- Centro Nacional de Gestión de Crisis de Lituania
- Agencia de Defensa Psicológica de Suecia
- Centro de Compromiso Global de Estados Unidos

Grupo de trabajo

Grupo de expertos en su calidad de funcionarios públicos, creado para proporcionar asesoramiento técnico coordinado al gobierno sobre cómo abordar amenazas específicas planteadas por la desinformación y/o desarrollar medidas dirigidas para mejorar la integridad de la información.

Dentro de un mismo país se pueden crear diferentes grupos de trabajo de carácter permanente o temporal, lo que permite realizar intervenciones y trabajos técnicos más eficaces frente a, por ejemplo, la manipulación de la información en unas elecciones o las campañas de salud pública.

Al tener una función similar a la de un grupo de trabajo, también se puede establecer un comité asesor, en el que generalmente participan expertos externos al gobierno.

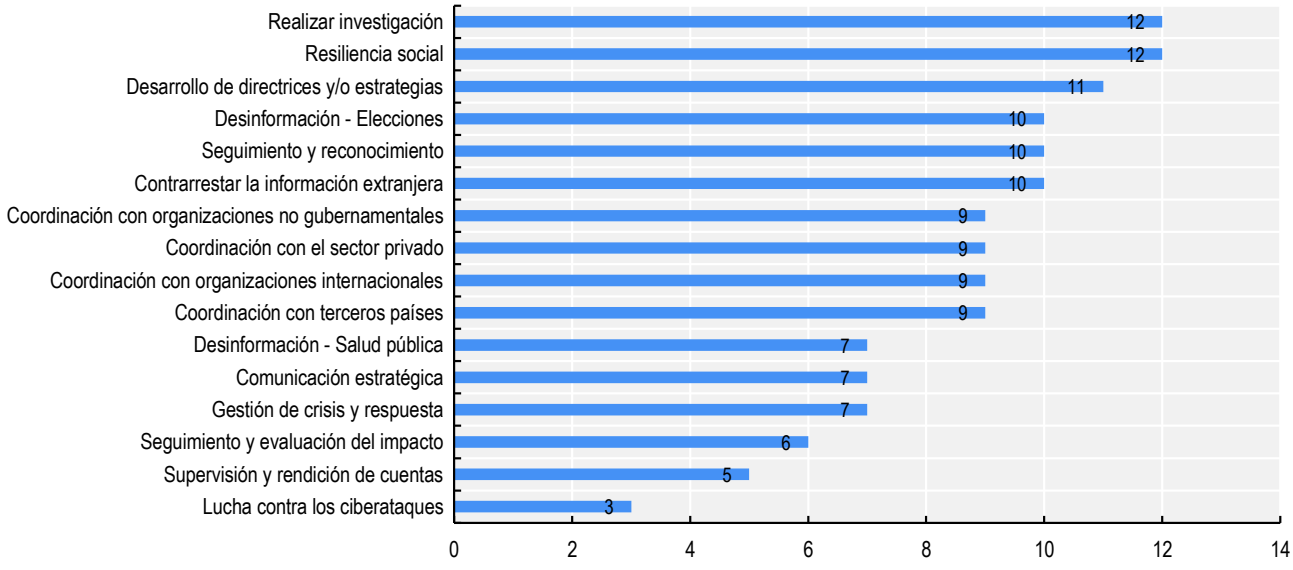
Los ejemplos incluyen:
- El Grupo de Trabajo de Garantía de la Integridad Electoral de Australia
- El Grupo de trabajo de Canadá sobre las amenazas a las elecciones en materia de seguridad e inteligencia (SITE)

Fuente: elaboración de los autores.

Cabe destacar que la formación de mecanismos de coordinación es un esfuerzo relativamente reciente, ya que todos ellos se han creado, por lo menos en su forma actual, desde 2016. Dadas las tendencias recientes en la desinformación, los gobiernos han tenido dificultades para definir su papel a la hora de abordar tales amenazas. El establecimiento de oficinas o mecanismos oficiales ha ayudado a los gobiernos democráticos a comprender y responder a estas amenazas, incluso proporcionando claridad sobre los tipos exactos de comportamiento y contenido a los que las agencias gubernamentales deben responder (Kleis Nielsen, 2021[6]). Los grupos de coordinación también crean puntos focales dentro de los gobiernos, que promueven la transparencia para ayudar a gestionar el riesgo de que las medidas diseñadas para combatir la desinformación exacerben la desconfianza social y mitiguen los efectos indeseados sobre la libertad de expresión y de opinión (Butcher, 2019[7]).

Los mecanismos de coordinación establecidos comparten a grandes rasgos objetivos prioritarios en relación con la realización de investigaciones sobre la dinámica de la desinformación, el aumento de la resiliencia social a la difusión de información falsa y engañosa, y el desarrollo o el aumento de la relevancia de las directrices y/o documentos estratégicos (Figura 4.3).

Figura 4.3. Objetivos del mecanismo de coordinación intergubernamental



Nota: núm.= 13 países.
Fuente: Encuesta de la OCDE sobre arquitectura institucional y prácticas de gobernanza para fortalecer la integridad de la información (2023).

Unidades de coordinación intergubernamental

Con respecto a los mecanismos de coordinación intergubernamental, las respuestas a las encuestas y a la información pública disponible sugieren que, por lo general, los países han desarrollado marcos legales que definen los parámetros dentro de los cuales pueden operar estos mecanismos. Estas disposiciones legales son especialmente importantes para explicar el alcance de la acción del mecanismo de coordinación, para establecer controles internos y procedimientos de presentación de informes para sus actividades y para reducir el riesgo de un posible abuso de las medidas de política pública.

De hecho, los mecanismos y unidades de coordinación intergubernamental deben tener unos mandatos claros y se les debe impedir expresamente intervenir en ámbitos de políticas, que pudieran poner en peligro la libertad de expresión y socavar la calidad democrática. Para ello, en mayo de 2023, Letonia aprobó los estatutos del Grupo de Coordinación Nacional sobre Seguridad del Espacio de la Información. Estos estatutos definen las normas jurídicamente vinculantes, que el mecanismo utiliza para operar y establecen el Departamento de Coordinación de Comunicación Estratégica de la Cancillería del Estado como la autoridad de gestión central (Recuadro 4.3).

Recuadro 4.3. El Grupo de Coordinación Nacional sobre Seguridad del Espacio de la Información – Letonia

El Grupo de Coordinación Nacional de la Seguridad del Espacio de Información es un órgano consultivo, que facilita la cooperación y el intercambio de información entre las instituciones encargadas de responder y mitigar los riesgos y desafíos de seguridad correspondientes.

Dirigido por el Departamento de Coordinación de Comunicación Estratégica de la Cancillería del Estado (StratCom), este grupo tiene dos funciones principales: (i) coordinar y supervisar la implementación del Informe Conceptual sobre la Comunicación Estratégica Estatal y la Seguridad del Espacio de la Información para 2023-2027; y (ii) facilitar la detección, reducción y prevención de riesgos y amenazas al espacio de la información estatal y la seguridad pública.

Los organismos que forman parte de dicho grupo son: la Cancillería del Presidente, los Ministerios de Cultura, Relaciones Exteriores, Interior, Defensa, Justicia, Protección Ambiental y Desarrollo Regional, Finanzas, Transporte, Educación y Ciencia, Economía, la Oficina del Primer Ministro, el Servicio de Seguridad del Estado, la Policía Estatal, el Consejo Nacional de Medios de Comunicación Electrónicos, el Consejo de Medios de Comunicación Electrónicos Públicos, la Institución de Respuesta a Incidentes de Seguridad de las Tecnologías de la Información CERT.lv y la Oficina de Protección de la Constitución.

Fuente: Latvijas Vēstnesis (2023[8]), «Valsts informatīvās telpas drošības koordinācijas grupas nolikums», https://likumi.lv/ta/id/341811-valsts-informativas-telpas-drosibas-koordinacijas-grupas-nolikums.

Una función esencial es la necesidad de que los gobiernos respondan rápidamente y, a menudo, dentro del ciclo de noticias, especialmente durante las crisis, para garantizar que se comparta una información precisa y evitar que arraiguen los contenidos falsos o engañosos. Las estructuras de crisis informativas son una herramienta importante en este sentido. En Lituania, la Estrategia de Seguridad Nacional estableció la creación del Centro Nacional de Gestión de Crisis (NKVC) como centro de referencia y de situación para coordinar las respuestas a las amenazas a la seguridad nacional, incluida la desinformación (Recuadro 4.4).

Recuadro 4.4. El Centro Nacional de Gestión de Crisis – Lituania

Desde 2017, las amenazas de desinformación dirigidas a Lituania han sido gestionadas por la Cancillería del Gobierno, tal y como establece la Estrategia de Seguridad Nacional del país. En 2022, se creó el Centro Nacional de Gestión de Crisis (NCMC) como el organismo encargado de la coordinación de la prevención y la gestión de crisis, incluida la respuesta del Estado a la desinformación a nivel nacional. En caso de crisis o de situaciones de emergencia, el Centro propone respuestas y soluciones, asiste a su implementación y facilita la coordinación interinstitucional.

Dentro del NCMC hay un Grupo de Trabajo de Coordinación de la Comunicación Estratégica coordina la comunicación estratégica en cuestiones de seguridad nacional a través de:

- Un grupo de trabajo intergubernamental (consistente en reuniones semanales y chats de Signal)
- Cooperación con los municipios (mediante chats de Signal).
- Participación de la sociedad civil y expertos académicos (reuniones trimestrales y chats de Signal)
- Interacción con los medios de comunicación (mediante chats de Signal)

Este modelo se probó con éxito durante la cumbre de la OTAN de 2023 celebrada en Vilna. Para formalizar y fortalecer el modelo, el NCMC creará en 2024 un modelo intergubernamental de seguimiento, evaluación e intercambio de información, compuesto por 10 instituciones gubernamentales, y desarrollará una estrategia de comunicación estratégica en el ámbito de la seguridad nacional.

Fuente: Departamento de Seguridad del Estado de Lituania (2022[9]), Evaluación de amenazas, https://www.vsd.lt/en/threats/threats-national-security-lithuania/; Gobierno de la República de Lituania (2023[10]), «Lithuania's new crisis management model presented at Baltic States Centres of Government Meeting», https://lrv.lt/en/news/lithuanias-new-crisis-management-model-presented-at-baltic-states-centres-of-government-meeting/.

Otros países han establecido organismos de coordinación a nivel nacional con un alcance que se centra en detectar y caracterizar las operaciones de desinformación orquestadas por agentes extranjeros. El Servicio de Vigilancia y Protección contra las Interferencias Digitales Extranjeras de Francia (VIGINUM) (Recuadro 4.5), la Agencia de Defensa Psicológica de Suecia (Recuadro 4.6) y el Centro de Compromiso Global de Estados Unidos (Recuadro 4.7) tienen mandatos limitados a la amenaza de la manipulación informativa y la injerencia por parte de agentes extranjeros. En estos casos, se hace una clara distinción con respecto a la procedencia (nacional/externa) de las amenazas de desinformación. Además, el Ministerio francés para Europa y de Asuntos Exteriores ha creado una unidad dedicada a supervisar las operaciones de desinformación contra la red diplomática francesa.

Recuadro 4.5. El Servicio de Vigilancia y Protección contra las Interferencias Digitales Extranjeras – Francia

El Servicio francés de Vigilancia y Protección contra las Interferencias Digitales Extranjeras (VIGINUM) fue creado en el seno de la Secretaría General de Defensa y Seguridad Nacional (SGDSN) mediante el Decreto núm. 2021-922 de 13 de julio de 2021, que establece sus misiones.

La tarea de esta agencia nacional es detectar y caracterizar, mediante el análisis de los contenidos en línea de acceso público, la manipulación extranjera de información en línea, que pudiera afectar a cuestiones fundamentales del interés nacional (integridad territorial, seguridad, diplomacia y funcionamiento de sus instituciones, etc.). También analiza sus efectos y coordina la protección del Estado contra dichas operaciones.

En este sentido, VIGINUM asiste al SGDSN en la coordinación de una red interministerial de administraciones y servicios con capacidades técnicas en el campo de la manipulación de la información y la interferencia digital extranjera. Asimismo, colabora estrechamente con los servicios y las administraciones que contribuyen directa o indirectamente a la lucha contra la manipulación de la información para detectar e investigar operaciones maliciosas. Cuando se detectan operaciones malintencionadas, la investigación de código abierto de VIGINUM respalda las contramedidas mediante el uso de la comunicación pública destinada a restaurar la confianza pública, comprometiéndose con otros ministerios (incluido el Ministerio para Europa y de Asuntos Exteriores, el Ministerio del Interior, el Ministerio de las Fuerzas Armadas, etc.) y con las autoridades responsables del buen desarrollo de las elecciones durante los períodos electorales. Sobre la base de la investigación de VIGINUM, Francia también ha expuesto públicamente numerosas campañas de interferencia digital extranjera

A nivel internacional, VIGINUM participa en intercambios regulares con homólogos internacionales, tanto bilateralmente como en el contexto de marcos multilaterales, como el Sistema de Alerta Rápida y el Mecanismo de Respuesta Rápida del G7.

Un elemento fundamental de VIGINUM es que opera dentro de un marco legal y ético riguroso, definido específicamente por el Decreto núm. 2021-1587 de 7 de diciembre de 2021. Este último es el resultado de consultas con representantes parlamentarios y del trabajo legal con el Consejo de Estado francés, basado en su autorización para consultar, recopilar y utilizar de manera automatizada datos personales disponibles públicamente en línea. El control de la gestión de los datos personales recopilados en línea está supervisado por la CNIL (Comisión Nacional francesa de Tecnologías de la Información y Libertades Civiles). Además, se ha creado un comité ético y científico adjunto a la SGDSN para seguir las actividades de VIGINUM. Un representante del más alto tribunal administrativo francés (el Consejo de Estado francés) preside el comité, compuesto por representantes cualificados de los ámbitos de la diplomacia, las fuerzas del orden, la ciencia y los medios de comunicación.

Fuente: SGDSN (2022[11]), Service de vigilance et protection contre les ingérences numériques étrangères "VIGINUM", https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques.

Recuadro 4.6. La Agencia Sueca de Defensa Psicológica – Suecia

En enero de 2022, Suecia creó la Agencia Sueca de Defensa Psicológica, un organismo gubernamental dependiente del Ministerio de Defensa, que identifica, analiza y contrarresta las actividades extranjeras de influencia maliciosa de la información y otras operaciones de desinformación dirigidas a Suecia o a sus intereses.

El objetivo de la defensa psicológica es salvaguardar las libertades fundamentales y la independencia de Suecia, a través de una sociedad abierta y democrática, y la libre formación de opinión. La agencia resalta que el gobierno debe garantizar que haya una conciencia pública sobre las amenazas informativas, sin afectar a las libertades de expresión y de opinión. Este enfoque preventivo se centra principalmente en el pensamiento crítico y en la educación para construir defensas sociales contra la desinformación, de modo que los actores maliciosos encuentren un entorno menos favorable para llevar a cabo sus actividades de influencia de la información.

La agencia está organizada en tres departamentos: administración, operaciones y desarrollo de capacidades. En colaboración con otras agencias gubernamentales, sus tareas principales son:

- Elaborar informes y análisis relacionados con determinadas situaciones, actores de amenazas y vulnerabilidades sociales, así como proponer las contramedidas adecuadas.
- Desarrollar métodos y tecnologías para identificar y contrarrestar las actividades de influencia extranjera maliciosa de la información.
- Desarrollar y fortalecer la capacidad social general de Suecia en términos de defensa psicológica. Esto incluye proporcionar apoyo a la población sueca, los organismos gubernamentales, los municipios, los medios de comunicación, las organizaciones de defensa voluntaria y la sociedad civil, así como facilitar una mayor coordinación entre estos actores.
- Apoyar acciones formativas y de desarrollo de conocimientos, por ejemplo, iniciando y financiando investigaciones relacionadas con la defensa psicológica.

Fuente: Agencia Sueca de Defensa Psicológica (2023[12]), Sitio web de la Agencia Sueca de Defensa Psicológica , https://www.mpf.se/en/about-us/.

Recuadro 4.7. El Centro de Compromiso Global – Estados Unidos

El Centro de Compromiso Global (GEC) del Departamento de Estado de Estados Unidos fue creado en 2016 en el seno del Departamento de Estado mediante la Orden Ejecutiva 13721. Su misión es liderar los esfuerzos del gobierno estadounidense para reconocer, comprender, exponer y contrarrestar la propaganda y la desinformación de estados y de actores no estatales extranjeros, destinados a socavar o influir en las políticas, la seguridad o la estabilidad de Estados Unidos, sus aliados y países socios. El GEC desarrolla su actividad en cinco ámbitos:

- Análisis e investigación: Los analistas y científicos de datos del GEC recopilan datos de actores estatales y no estatales extranjeros para producir análisis sobre sus narrativas, tácticas y técnicas de influencia maliciosa de la información.
- Asociaciones internacionales: El GEC ha creado y participa en numerosas coaliciones y asociaciones internacionales con otros gobiernos nacionales con el objetivo de coordinar análisis y acciones contra la desinformación, y reforzar conjuntamente la integridad del entorno informativo global.
- Programas y campañas: El GEC adapta sus iniciativas a los desafíos específicos de entornos informativos únicos en el extranjero y las coordina internamente dentro del Departamento de Estado y con socios

interinstitucionales e internacionales, para fomentar la resiliencia social e institucional frente a los esfuerzos de propaganda y de desinformación extranjeras en el exterior.

- Exposición: El GEC desempeña un papel de coordinación en las acciones interinstitucionales destinadas a exponer las operaciones extranjeras de influencia de la información, incluido el uso de sitios proxy y de redes sociales en el extranjero.
- Evaluación tecnológica y compromiso: El GEC identifica, evalúa y prueba el uso de tecnologías para contrarrestar la desinformación y la propaganda extranjera en el extranjero, así como para reducir los riesgos que plantea el uso de los medios generados mediante IA en la manipulación de la información por parte de actores maliciosos extranjeros, mediante el intercambio de conocimientos entre los departamentos y las agencias gubernamentales de EE. UU. y de socios internacionales.

Fuente: Departamento de EE. UU. (n.d.[13]), "About Us – Global Engagement Center", https://www.state.gov/about-us-global-engagement-center-2/ (estado a 31 de agosto de 2023).

La función de comunicación pública también ha desempeñado un papel destacado en la coordinación de los esfuerzos para responder a las amenazas de la desinformación. Si se gestiona adecuadamente y se le asignan los recursos necesarios, esta función puede desempeñar un papel importante en los esfuerzos de los gobiernos para fortalecer la conciencia sobre el estado de las amenazas informativas y promover una coordinación eficaz de la respuesta. Con ese fin, la función de comunicación pública debería basarse en esfuerzos dirigidos a promover el bien público, realizarse de una manera transparente y estar guiada por mandatos claros, que separen las actividades de comunicación política y pública. En ese contexto, el Ministerio francés para Europa y de Asuntos Exteriores realizó, por ejemplo, en 2023 y 2024 tres campañas de divulgación pública basadas en investigaciones de VIGINUM con la publicación de un informe técnico, que comparte los datos de fuentes abiertas, que ayudaron a las autoridades francesas a llegar a la conclusión de que la interferencia digital extranjera había tenido como objetivo al país.

La Encuesta de la OCDE sobre la comprensión de la comunicación pública de 2020 encontró que el 64 % de los 46 países encuestados indicaron que había estructuras, equipos o individuos específicos, que participaban en los esfuerzos de comunicación pública relacionados con la lucha contra la desinformación (OECD, 2021[14]). El enfoque en la lucha contra la desinformación a través de la función de comunicación pública se expandió rápidamente durante la pandemia de COVID-19, ya que los gobiernos intentaron contrarrestar las falsas narrativas de rápida propagación sobre las causas del virus y las curas sin base médica.

En lo que respecta a la comunicación pública, la capacidad centralizada podría ser útil para producir recursos comunitarios, compartir información y desarrollar una respuesta pública coherente para las agencias y los ministerios a nivel nacional. En el Reino Unido, la arquitectura de las respuestas de comunicación pública ha surgido como resultado de intervenciones y enfoques diseñados para enfrentarse a varias olas de desinformación. Por ejemplo, la Unidad de Lucha contra la Desinformación (CDU) lidera acciones continuar para monitorear y marcar los contenidos falsos y engañosos, ya sea para impulsar su desmentido o para colaborar con las plataformas en línea. Además, la Célula de Información Gubernamental (GIC) fue creada, en el seno de la Oficina de Relaciones Exteriores, Commonwealth y Desarrollo (FCDO), en vísperas de la invasión a gran escala de Ucrania por parte de Rusia con la misión de contrarrestar las operaciones de información de actores hostiles, que representan amenazas para la seguridad, la política exterior y las instituciones democráticas del Reino Unido (OECD, 2023[15]).

Otros ejemplos de oficinas de este tipo son las centradas en la implementación de iniciativas y políticas específicas diseñadas para contrarrestar la desinformación mediante el fortalecimiento del espacio mediático y la información en general. Este es el enfoque adoptado, por ejemplo, en Italia a través del Departamento de Información y Publicaciones (véase Recuadro 4.8).

Recuadro 4.8. El papel del Departamento de Información y Publicaciones en Italia

En Italia, el Departamento de Información y Publicaciones, perteneciente a la Oficina del Primer Ministro bajo la responsabilidad política de un Secretario de Estado, supervisa el diseño y la implementación de políticas para proteger la libertad y el pluralismo de los medios, tanto para los medios tradicionales (editoriales, periódicos y revistas) como para los medios digitales, al tiempo que garantiza la salvaguarda de los derechos de autor. Contrarrestar la desinformación se ha convertido en uno de los objetivos definitorios de este Departamento, puesto que está centrado en garantizar un ecosistema informativo profesional, independiente y diverso, así como el libre flujo de información fidedigna.

Una de las principales actividades del Departamento es proporcionar apoyo financiero a los medios profesionales para fomentar el pluralismo de la información (véase el Capítulo 2). La sostenibilidad financiera es un desafío acuciante para el periodismo de calidad, ya que tanto los editores tradicionales como los digitales se enfrentan a graves limitaciones de financiación. El nuevo Fondo para el Pluralismo y la Innovación Digital de la Información y la Publicación de Medios sustituye todos los mecanismos permanentes y puntuales anteriores e incorpora el apoyo financiero público al ecosistema de los medios de comunicación. El objetivo de este organismo es fortalecer la calidad y la fiabilidad de la información proporcionar incentivos para aumentar el número de periodistas profesionales, incluso a través de productos mediáticos innovadores y de inversiones en nuevos contenidos y nuevas tecnologías.

El Departamento de Información y Publicaciones también apoya la implementación de la Estrategia Nacional de Ciberseguridad (2022-2026). Como coordinador nacional de la medida para prevenir y combatir la desinformación en línea, este Departamento se centra en dos proyectos: a) mejorar la alfabetización mediática de los ciudadanos, incluso a través de campañas de información sobre posibles usos nocivos de la inteligencia artificial; y b) desarrollar un conocimiento profundo de las amenazas relevantes, en asociación con las universidades, para emitir directrices que apoyen la función de comunicación pública.

Además, el Departamento ha creado un Comité de Expertos encargados de analizar el impacto de la IA generativa en el sector de la información y la edición. El informe de 2024 del Comité pone de relieve el riesgo percibido que plantea la inteligencia artificial para la propagación de la desinformación; el amplio apoyo para establecer alianzas estables entre múltiples partes interesadas para el intercambio de información fiable y de calidad entre los ciudadanos, las instituciones públicas y los medios de comunicación; la necesidad de proteger el empleo de periodistas y defender la profesionalidad del sector; y recomendaciones para proteger el espacio democrático contra la interferencia y la manipulación extranjeras por parte de actores maliciosos.

Fuente: Artículo 1 apdo. 315 de la Ley núm. 213 de 2023 (Ley de Presupuestos para 2024); Artículo 17 del Decreto-ley núm. 198 de 2022, convertido en Ley núm. 14 de 2023 y Decreto del Presidente del Consejo de Ministros de 11 de julio de 2023; Medida #24 del Plan de Implementación de la Estrategia Nacional de Ciberseguridad; Decreto de la Subsecretaría de Estado responsable de información y publicaciones de 23 de octubre de 2023.

Grupos de trabajo especializados

Además de crear unidades centrales para coordinar las respuestas a la desinformación, los gobiernos también pueden considerar la creación de grupos de trabajo especializados, compuestos por funcionarios de toda la administración pública o socios externos para asesorar sobre las respuestas políticas. Estos grupos de trabajo pueden ser de naturaleza permanente o temporal. Es importante tener en cuenta que se pueden establecer diferentes unidades de expertos dentro del mismo país para permitir unas intervenciones y un trabajo técnico más receptivos cuando hay objetivos específicos en juego.

Alemania ha adoptado una configuración específica, con un ministerio que dirige la política nacional sobre la desinformación, complementada por una red de grupos de trabajo interministeriales y grupos de trabajo que cooperan en prioridades temáticas específicas (Recuadro 4.9).

Recuadro 4.9. Grupos de trabajo interministeriales para contrarrestar la desinformación – Alemania

Dentro del Gobierno Federal de Alemania, el Ministerio Federal del Interior y la Patria (BMI) se encarga de la coordinación estratégica en relación con las amenazas de la desinformación. Alemania también ha creado grupos de trabajo especiales compuestos por funcionarios de diferentes ministerios a nivel nacional y federal, y servicios de inteligencia.

El BMI preside un grupo de trabajo interministerial sobre amenazas híbridas creado en 2018 para hacer frente a la manipulación de la opinión pública a través de la difusión de desinformación y propaganda en línea, el espionaje y los ciberataques a infraestructuras críticas, entre otras amenazas.

Cuando comenzó la guerra de agresión de Rusia contra Ucrania, se creó un grupo especial dentro de este grupo de trabajo, para centrarse en las actividades de desinformación rusas. El BMI junto con el Ministerio Federal de Relaciones Exteriores (AA), la Oficina de Prensa e Información del Gobierno Federal y los servicios nacionales de inteligencia supervisan cuidadosamente el espacio de la información para identificar las narrativas rusas. También dedican esfuerzos en reforzar la comunicación proactiva y basada en hechos, proporcionando actualizaciones sobre la situación y fomentando un enfoque más crítico de la información y las fuentes, especialmente, las de las redes sociales. El BMI se centra en la desinformación orquestada por estados o actores extranjeros para influir en la opinión pública y se esfuerza por fortalecer la resiliencia social. El Gobierno Federal también participa en conversaciones regulares e intensivas con socios internacionales, tanto bilateralmente como en el contexto de la Unión Europea, el G7 y la OTAN.

Fuente: Ministerio Federal del Interior y la Patria (2023[16]), "Measures taken by the Federal Government to fight disinformation", https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation/measures-taken-by-the-federal-government.html.

En Chile se creó en 2023 una «Comisión Nacional contra la Desinformación» como comité asesor para asesorar al Ministerio de Ciencia, Tecnología, Conocimiento e Innovación y a la Secretaría General de Gobierno (*Segegob*) sobre de los efectos de la desinformación en la calidad democrática de las plataformas digitales, la alfabetización digital y las buenas prácticas digitales (Recuadro 4.10).

Recuadro 4.10. Comisión Nacional contra la Desinformación de Chile

La Comisión Nacional Contra la Desinformación de Chile fue creada en mayo de 2023 mediante decreto oficial en el seno del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación. El objetivo de este organismo temporal es asesorar al Ministro de Ciencia, Tecnología, Conocimiento e Innovación, y al Ministro Secretario General de Gobierno, en asuntos relacionados con el fenómeno global de la desinformación y su manifestación en Chile. La comisión está compuesta por 9 miembros que representan a universidades públicas y privadas, ONG, fundaciones y organizaciones de verificación de hechos. La Comisión debe entregar dos informes en el plazo de un año: el primero para analizar las amenazas de desinformación y el segundo para proporcionar directrices y recomendaciones para la formulación de las políticas públicas pertinentes.

Fuente: Ministerio de Ciencia, Tecnología, Conocimiento e Innovación (n.d.[17]), "Comisión Asesora contra la Desinformación", https://www.minciencia.gob.cl/areas/comision-contra-la-desinformacion/.

Los países también han establecido consultas y evaluaciones periódicas para garantizar que las respuestas políticas se adapten a la evolución del espacio de la información. Por ejemplo, la Unidad de Protección de la Democracia de la Oficina del Consejo Privado de Canadá creó recientemente un grupo interdepartamental para identificar lagunas políticas en el enfoque del Gobierno canadiense sobre la desinformación, así como un grupo interdepartamental de coordinación de la investigación que garantice unos esfuerzos de investigación completos y bien alineados sobre el tema.

Finalmente, incluso en los casos en los que los países no hayan establecido un mecanismo de coordinación entre todos los niveles de gobierno dedicado a contrarrestar la desinformación o a fomentar la integridad de la información en general, los gobiernos podrían establecer grupos de trabajo formados por personal de diferentes oficinas, como el Centro de Gobierno (Gabinete u Oficina de la Presidencia) y ministerios o departamentos de asuntos exteriores, comunicación estratégica, sanidad, educación, cultura, defensa y políticas digitales, especialmente, cuando se responde a prioridades temáticas específicas. Por ejemplo, en 2023, Brasil estableció un Comité interministerial para combatir la desinformación relacionada con las Políticas Nacionales de Inmunización y Salud Pública. El objetivo del Comité es aportar un enfoque estratégico e integrado para orientar al Ministerio de Salud en el desarrollo y la evaluación de la comunicación pública en torno a los problemas de salud, intercambiar información entre el gobierno sobre la desinformación relacionada con las políticas de salud pública y desarrollar las investigaciones, los recursos y las formaciones correspondientes para apoyar los esfuerzos del gobierno en la lucha contra la desinformación en este espacio. El Comité está integrado por representantes de la Secretaría de Comunicación Social de la Presidencia de la República, la Fiscalía General de la República, la Contraloría General de la República, el Ministerio de Ciencia, Tecnología e Innovación, el Ministerio de Justicia y Seguridad Pública y el Ministerio de Salud (Government of Brazil, 2023[18]).

Las experiencias de los países en el establecimiento de mecanismos de coordinación hasta la fecha sugieren que los gobiernos aprecian cada vez más el valor de los esfuerzos organizados y coherentes para contrarrestar las amenazas de la desinformación y mejorar la integridad de la información. Las iniciativas también inciden en la importancia de que las oficinas eviten la politización y las restricciones a la libertad de expresión, permitiendo al mismo tiempo la difusión eficaz y oportuna de la información de inteligencia entre las autoridades competentes (tanto a nivel local como federal y nacional) y, potencialmente, los socios externos. Los esfuerzos para garantizar un funcionamiento sólido y sostenible de los mecanismos de coordinación también apuntan a la importancia de establecer mandatos claros, entre otras cosas, definiendo las amenazas de desinformación que el mecanismo u oficina pretende abordar.

4.2.3. La coordinación y la cooperación internacional son esenciales en la lucha contra la desinformación

Como los flujos de información no conocen fronteras en el mundo globalizado y digitalizado actual, la cooperación y la coordinación internacionales son un elemento esencial para diseñar respuestas políticas a la altura del desafío de la integridad de la información. La naturaleza transnacional de este desafío también se pone de manifiesto en el uso de la manipulación de la información por parte de actores maliciosos extranjeros para interferir en los asuntos nacionales. De hecho, la ausencia de participación en diálogos transnacionales podría animar a los estados hostiles a utilizar un enfoque fragmentado en su propio beneficio (Pamment, 2020[19]). La información falsa y engañosa también puede tener efectos negativos transfronterizos en cuestiones relacionadas con la salud pública, las comunidades minoritarias y el cambio climático (Lewandowsky, 2021[20]; UNDP, 2021[21]). En este contexto, al igual que en otros ámbitos de la economía digital, la cooperación normativa internacional debería formar parte del conjunto de instrumentos políticos destinados a responder a las amenazas de la desinformación y a reforzar la integridad de la información.

Por lo tanto, los países están colaborando y coordinando sus acciones a nivel internacional para reforzar su capacidad de contrarrestar estas amenazas. De hecho, las respuestas nacionales son más eficaces cuando se basan en el conocimiento y la experiencia de otros países que se enfrentan a problemas similares. Por lo tanto, la mejora de la coordinación interna facilitará los esfuerzos de los países para participar y comprometerse en iniciativas internacionales, cuya

misión es prevenir y contrarrestar las actividades de desinformación (Jeangène Vilmer, 2021[22]).

Existen numerosos foros internacionales y mecanismos de coordinación, cada uno de los cuales presenta diferentes configuraciones de alianzas de países y prioridades temáticas. Las organizaciones internacionales, los grupos especializados o ad hoc, las convocatorias dirigidas por los gobiernos y los acuerdos marco son los principales métodos mediante los cuales los países se involucran en estos temas de manera bilateral y multilateral. A pesar de la amplitud y la diversidad de las opciones de coordinación internacional, el 90 % de los encuestados indicaron que el refuerzo de la cooperación con los países socios es un área prioritaria de mejora en la lucha contra las amenazas de la desinformación.

En primer lugar, las organizaciones internacionales continúan desarrollando sus esfuerzos para ayudar a los países a reforzar la integridad de la información. Por ejemplo, además del Centro de Recursos DIS/MIS de la OCDE,[6] que actúa como plataforma para el análisis de políticas y el diálogo entre los 38 países miembros y otros actores, la OCDE reúne a países miembros y no miembros a través de una serie de iniciativas y redes. Estas iniciativas se centran en temas como la inteligencia artificial,[7] la exploración y la promoción de una gobernanza más eficaz para la integridad de la información en los países en desarrollo[8] y la presentación de informes de transparencia por parte de las plataformas en línea.[9] En conjunto, estas iniciativas de la OCDE contribuyen a la labor del Centro de Recursos DIS/MIS de la OCDE y al esfuerzo mundial por reforzar la integridad de la información.

La Secretaría de la OTAN y el Centro de Excelencia de Comunicaciones Estratégicas de la OTAN (OTAN StratCom COE, establecido en Letonia en 2014), analizan, investigan y apoyan las respuestas de comunicación estratégica a la propagación de la desinformación. EUvsDisinfo[10] es un proyecto del East StratCom Task Force del Servicio Europeo de Acción Exterior, creado en 2015, con el objetivo de pronosticar, abordar y responder mejor a las campañas de desinformación rusas que afectan a la Unión Europea, sus Estados miembros y otros países de la región (el impacto normativo transnacional de la UE se analiza más a fondo en el Capítulo II). Por último, el Centro Europeo de Excelencia para la Lucha contras las Amenazas Híbridas (Hybrid CoE) se estableció en Finlandia en 2017 para contrarrestar las amenazas híbridas y desarrollar las capacidades y la conciencia en los países participantes (Recuadro 4.11).

Recuadro 4.11. Centro Europeo de Excelencia para la Lucha contras las Amenazas Híbridas (Hybrid CoE)

Un centro internacional de expertos para optimizar las capacidades analíticas y las oportunidades de formación

El Hybrid CoE fue establecido en Helsinki en 2017 por los primeros nueve estados participantes, la OTAN y la Unión Europea. Su creación estuvo motivada por el deseo de desarrollar la resiliencia y las capacidades para contrarrestar las amenazas híbridas mediante la investigación, la formación práctica y los ejercicios, en los que participan representantes de los sectores privado, público, civil, militar y académico. Hoy en día, Hybrid COE cuenta con 33 estados participantes.

El término amenaza híbrida se puede definir como una acción realizada por actores estatales o no estatales para debilitar o dañar a los gobiernos democráticos influyendo en la toma de decisiones. Estas amenazas combinan medios militares y no militares, así como encubiertos y abiertos, incluida la desinformación, los ciberataques, la presión económica, la migración, el despliegue de grupos armados irregulares y el uso de fuerzas regulares. Dichas acciones están coordinadas y sincronizadas mediante el uso de una variedad de medios y están diseñadas para permanecer por debajo del nivel de detección y atribución (NATO, 2023[23]).

El Hybrid CoE participa activamente en una amplia gama de proyectos educativos y ejercicios de formación. En 2022, organizaron el Helsinki Countering Disinformation Wargame, un juego híbrido de simulación de amenazas centrado en la desinformación rusa y china y diseñado para ayudar a identificar lagunas y puntos fuertes en los sistemas de resiliencia de los países. El objetivo de estas simulaciones del mundo real es desarrollar mejores herramientas y técnicas para contrarrestar la desinformación y los planes de comunicación estratégica adaptados a las necesidades de los estados participantes del Hybrid CoE y los paisajes de amenazas.

Fuente: Hybrid CoE (n.d.[24]), "What is Hybrid CoE?", https://www.hybridcoe.fi/about-us/.

Por su parte, la UNESCO apoya a todos sus miembros a nivel mundial en el desarrollo de actividades de alfabetización mediática e informacional y en la mejora de la capacidad de los responsables políticos, educadores, periodistas y profesionales de los medios de comunicación, organizaciones juveniles y poblaciones desfavorecidas.[11] Además, la UNESCO ha elaborado unas Directrices para la Gobernanza de las Plataformas Digitales, un documento de alto nivel que tiene como objetivo «salvaguardar el derecho a la libertad de expresión en la gobernanza de las plataformas digitales, incluidos el acceso a la información y otros derechos humanos, al tiempo que se tratan aquellos contenidos que pueden restringirse lícitamente en virtud de la normativa internacional en materia de derechos humanos (UNESCO, 2023[25])». También perteneciente al sistema de las Naciones Unidas, el Programa de las Naciones Unidas para el Desarrollo (PNUD) explora la integridad de la información en relación con su mandato y las áreas temáticas de trabajo. A nivel programático, el PNUD proporciona orientación práctica para el diseño de programas.[12]

Más allá de la participación amplia de los miembros a través de organizaciones internacionales o de la Unión Europea, los gobiernos han establecido mecanismos de participación más específicos para abordar aspectos de la lucha contra la desinformación. Estados Unidos presentó recientemente una nueva herramienta para generar consenso internacional en torno a un enfoque común sobre la desinformación y la manipulación de la información por actores extranjeros, y para proteger las sociedades libres y abiertas (para obtener información adicional, consulte Recuadro 4.12).

Recuadro 4.12. El Marco de referencia para contrarrestar la manipulación informativa por parte de adversarios extranjeros - Departamento de Estado de EE. UU.

El Marco para contrarrestar la manipulación informativa por parte de adversarios extranjeros fue anunciado por el Departamento de Estado de EE. UU. en enero de 2024 y está siendo implementado por el Centro de Compromiso Global. Su objetivo es desarrollar una comprensión común de esta amenaza y profundizar la cooperación entre socios afines, establecer un panorama operativo común y apoyar el desarrollo de ecosistemas de información resilientes y basados en hechos. Además, fomenta la alineación a lo largo de un conjunto común de ámbitos de acción para facilitar la generación de respuestas coordinadas frente a la manipulación informativa por parte de agentes extranjeros. Comprende cinco ámbitos de acción clave:

1. Estrategias y políticas nacionales
2. Estructuras e instituciones de gobernanza
3. Capacidad humana y técnica
4. Sociedad civil, medios de comunicación independientes y mundo académico
5. Compromiso multilateral

Al comprometerse con estos cinco ámbitos de acción clave, los socios internacionales pueden mejorar la cohesión bilateral y multilateral para desarrollar la resiliencia social frente a la desinformación y la manipulación de la información por actores extranjeros.

Fuente: Departamento de Estado de EE. UU. (2024[26]), "The Framework to Counter Foreign State Information Manipulation", https://www.state.gov/the-framework-to-counter-foreign-state-information-manipulation/.

En cuanto al G7, por ejemplo, el mecanismo de respuesta rápida (G7 RRM) es un mecanismo para reforzar la coordinación, con el fin de identificar y responder a diversas y cambiantes amenazas extranjeras a la democracia. Creado en 2018, comprende los Puntos Focales de los Miembros del G7 e incluye a la Unión Europea, la OTAN, Australia, Nueva Zelanda, los Países Bajos y Suecia como observadores (véase Recuadro 4.13).

Recuadro 4.13. El mecanismo de respuesta rápida del G7

El mecanismo de respuesta rápida del G7 (G7 RRM) fue establecido por los Líderes del G7 en la Cumbre de 2018 celebrada en Charlevoix. El equipo del mecanismo de respuesta rápida de Global Affairs Canada (RRM Canada) funciona como su secretaría permanente. La misión del G7 RRM es fortalecer la coordinación entre los países del G7 para identificar y responder a las diversas y cambiantes amenazas extranjeras a la democracia. Esto se logra mediante el fortalecimiento de los medios de comunicación y del entorno informativo, respondiendo a las amenazas extranjeras a los derechos y libertades de los ciudadanos y promoviendo la seguridad de las elecciones. Los puntos focales del G7 RRM se reúnen mensualmente para compartir información, mejores prácticas y lecciones aprendidas.

Fuente: Mecanismo de respuesta rápida de Canadá: Global Affairs Canada, https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/index.aspx?lang=eng.

El Triángulo de Lublin fue creado por Polonia, Lituania y Ucrania para establecer una cooperación trilateral destinada a contrarrestar las campañas de desinformación rusas. Estos tres países han trabajado juntos para identificar narrativas, mensajes y tácticas específicos utilizados en su contra; analizar el grado de resiliencia social a la propaganda del gobierno ruso; y hacer recomendaciones para abordar mejor las amenazas que van surgiendo (Recuadro 4.14).

Recuadro 4.14. El Triángulo de Lublin – Cooperación trilateral para combatir la desinformación rusa

En julio de 2020, los Ministros de Asuntos Exteriores de Polonia, Lituania y Ucrania crearon el Triángulo de Lublin (L3), una iniciativa regional destinada a fortalecer la cooperación militar, cultural, económica y política mutua basada en lazos y tradiciones históricas. En 2021, los países del L3 firmaron una Hoja de Ruta, que establece las direcciones clave para ampliar la cooperación, incluyendo actividades estratégicas conjuntas para responder a las amenazas híbridas, contrarrestar la desinformación y reforzar la resiliencia de la sociedad. El trabajo del Triángulo de Lublin se rige por un Plan de Acción Conjunto para Combatir la Desinformación para 2022-2023.

Fuente: Instytut Kościuszki (2022[27]), Report – Resilience to Disinformation, https://ik.org.pl/en/.

Los gobiernos también han establecido diversos encuentros y marcos de trabajo, que facilitan el debate, fijan prioridades para el futuro y marcan una dirección común de actuación. Por ejemplo, Estados Unidos estableció y organizó las dos primeras reuniones de la Cumbre para la Democracia (en diciembre de 2021 y marzo de 2023, respectivamente), mientras que la tercera fue organizada por la República de Corea en marzo de 2024. En las dos primeras Cumbres participaron en torno a 100 gobiernos y la Cumbre para la Democracia de 2023 tuvo como tema principal la integridad de la información, prestando especial atención a los temas relacionados con la cooperación internacional, la alfabetización informacional y las definiciones.[13]

Siguiendo la estela del Grupo de Trabajo sobre Integridad de la Información de la Cumbre por la Democracia, los gobiernos de Canadá y los Países Bajos lanzaron en septiembre de 2023 la Declaración Mundial sobre Integridad de la Información en Línea. Esta declaración establece «una serie de compromisos internacionales de alto nivel para proteger y promover la integridad de la información en línea... y pretende reforzar los esfuerzos multilaterales existentes para proteger el ecosistema informativo» (Government of the Netherlands, 2023[28])" (véase Recuadro 4.15).

Recuadro 4.15. La Declaración Global sobre la Integridad de la Información en Línea

La Declaración Global sobre la Integridad de la Información en Línea, lanzada en septiembre de 2023 y firmada por 34 países, establece los compromisos internacionales de los estados participantes para proteger y promover la integridad de la información en línea. También establece expectativas para que el sector privado y las plataformas en línea empleen prácticas comerciales, que contribuyan a un ecosistema de información saludable en línea. La Declaración está refrendada por: Australia, Austria, Bélgica, Brasil, Canadá, Chile, Costa Rica, República Checa, Dinamarca, República Dominicana, Estonia, Finlandia, Francia, Alemania, Georgia, Islandia, Irlanda, Japón, Kenia, Letonia, Lituania, Luxemburgo, Moldavia, Países Bajos, Nueva Zelanda, Macedonia del Norte, República de Corea, Suecia, Suiza, Reino Unido, Uruguay y Estados Unidos.

La Declaración define el término «integridad de la información» como un ecosistema informativo, que «produce información precisa, fidedigna y fiable, lo cual significa que las personas pueden confiar en la exactitud de la información a la que acceden, al tiempo que están expuestas a una variedad de ideas».

Los compromisos específicos asumidos por los estados participantes incluyen:

- Abstenerse y condenar las campañas de desinformación dirigidas por el Estado
- Respetar, promover y cumplir el derecho a la libertad de expresión
- Implementar la legislación correspondiente de acuerdo con el derecho internacional
- Evitar la restricción de la libertad de expresión con el pretexto de contrarrestar la desinformación
- Promover una educación cívica más sólida en línea y la alfabetización digital
- Apoyar a los medios de comunicación independientes, las noticias y el periodismo
- Adoptar medidas activas para abordar la desinformación dirigida a grupos en situaciones vulnerables.

La Declaración también insta a las plataformas en línea y a la industria que desempeñen un papel constructivo, respetando el estado de derecho, los derechos humanos y las libertades fundamentales; promoviendo la investigación; mejorando la transparencia; mejorando la supervisión de los algoritmos; y preservando la integridad electoral y democrática.

Fuente: Gobierno de los Países Bajos (2023[29]), Declaración Global sobre Integridad de la Información en Línea, https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2023/09/20/global-declaration-on-information-integrity-online.

Otro ejemplo de una plataforma para el diálogo multilateral es el Consejo UE-EE. UU. de Comercio y Tecnología, creado en 2021 para servir como un foro para que Estados Unidos y la Unión Europea se coordinen en cuestiones comerciales, económicas y tecnológicas mundiales. En la cuarta reunión ministerial del TTC en mayo de 2023, la Declaración Conjunta señaló la «profunda preocupación compartida por la manipulación informativa y la injerencia extranjera (FIMI), así como por la desinformación». También señaló la «oportunidad de desarrollar un estándar compartido para el intercambio de información sobre amenazas relacionadas con la FIMI» e incluyó un llamamiento a «mejorar la preparación de la comunidad de múltiples partes interesadas para intensificar sus acciones contra las amenazas de la FIMI, además de explorar la posibilidad de un mayor apoyo a la creación de capacidades en África, América Latina y los países vecinos de la UE (TTC, 2023[30])».

El Pacto por la Información y la Democracia es un acuerdo intergubernamental no vinculante firmado hasta la fecha por 52 países para promover e implementar principios democráticos en el espacio global de la información y la comunicación (véase Recuadro 4.16). La supervisión e implementación del Pacto está coordinada por el Foro sobre Información y Democracia, que es una entidad independiente sin fines de lucro dirigida por organizaciones de la sociedad civil. Este mandato del Foro de servir como un grupo independiente de la sociedad civil para apoyar al Paco ofrece importantes oportunidades de participación para que los socios gubernamentales y no gubernamentales se beneficien de los expertos y académicos convocados para evaluar el espacio global de información y comunicación, así como para desarrollar recomendaciones a las diferentes partes interesadas, que son quienes determinan cómo deben evolucionar las normas (Forum on Information and Democracy, 2023[31]).

Recuadro 4.16. Pacto por la Información y la Democracia

Firmado durante la 74.ª Asamblea General de la ONU en septiembre de 2019, el Pacto por la Información y la Democracia reafirma los siguientes principios:

1. El espacio global de información y comunicación, que es un bien público compartido de importante valor democrático, debe apoyar el ejercicio de los derechos humanos, en particular, el derecho a la libertad de opinión y de expresión, incluida la libertad de buscar, recibir y transmitir información e ideas de todo tipo a través de cualquier medio de comunicación de su elección e independientemente de las fronteras según lo previsto en el Pacto Internacional de Derechos Civiles y Políticos (artículo 19).

2. Se debe proteger y promover el acceso a una información fiable para permitir la participación democrática y el ejercicio de la libertad de opinión y de expresión.
3. Se considera que la información es fiable en la medida en que su recopilación, procesamiento y difusión sean libres e independientes, basados en la verificación cruzada de diversas fuentes y en un panorama mediático pluralista, donde los hechos pueden dar lugar a una diversidad de interpretaciones y puntos de vista.
4. De acuerdo con el derecho internacional y las normas sobre el derecho a la libertad de opinión y de expresión, los periodistas y trabajadores de los medios de comunicación en el ejercicio de sus funciones deberán estar protegidos contra toda forma de violencia, amenaza y discriminación, así como contra toda forma de detención arbitraria, procesos legales abusivos; contra cualquier intento excesivamente restrictivo de impedirles realizar su trabajo y de acceder a recursos legales adecuados, incluso en lo que respecta a la confidencialidad de sus fuentes.
5. Asimismo, se deben desarrollar modelos de negocio sostenibles para dar soporte a un periodismo independiente de alta calidad.

Fuente: Foro sobre Información y Democracia (n.d.[32]), "International Partnership for Information & Democracy", https://informationdemocracy.org/international-partnership-on-information-democracy/.

Cabe destacar que estos ejemplos no incluyen compromisos bilaterales ni la cooperación internacional centrados en cuestiones de inteligencia o de seguridad. Sin embargo, los países han señalado que participan en estas redes e iniciativas para beneficiarse del intercambio oportuno de información, la investigación de fertilización cruzada, la participación en actividades de desarrollo de capacidades y el intercambio de mejores prácticas, así como para el establecimiento de objetivos compartidos. Estos mecanismos también son clave para desarrollar una terminología común, compartir inteligencia estratégica y metodologías analíticas, mejorar la investigación y superar las divisiones políticas internas.

En el futuro, tanto los gobiernos como las organizaciones internacionales deberán seguir dando respuesta a los problemas nuevos y emergentes en el espacio de la información, evitando la superposición o duplicación de otras iniciativas (véase, por ejemplo, la Recomendación de la OCDE sobre la Cooperación Regulatoria Internacional para Abordar los Desafíos Globales (OECD, 2022[33])). Es necesario hacer más para garantizar un enfoque claro a la hora de aprovechar las oportunidades que ofrecen las perspectivas únicas, la membresía y los mandatos de las organizaciones correspondientes, así como para coordinar la acción global compartida.

4.3. UN ESPACIO DE INFORMACIÓN CAMBIANTE EXIGE UNA MAYOR ATENCIÓN AL DESARROLLO DE CAPACIDADES EN LA ADMINISTRACIÓN PÚBLICA

El desarrollo de la capacidad colectiva del gobierno para ayudar en la lucha contra la desinformación comienza con los funcionarios públicos que se enfrentan a estas amenazas en su trabajo diario. El nivel de sofisticación de las campañas de desinformación requiere una mejora de las competencias y una labor de formación en todos los niveles de gobierno, para garantizar que los cargos electos y los responsables políticos posean los conocimientos y las herramientas necesarios para reconocer, monitorear y contrarrestar la difusión de información falsa y engañosa sin constreñir los derechos humanos y las libertades fundamentales. Los esfuerzos de desarrollo de capacidades también deben diseñarse con el objetivo más amplio de fomentar el pensamiento crítico y aumentar la conciencia de los funcionarios públicos sobre los riesgos de la desinformación. Esto también es importante para contribuir a evitar la difusión de narrativas falsas. Con ese fin, la participación de las escuelas nacionales de administración pública u oficinas especializadas, como la Oficina de Integridad de Bélgica, puede contribuir a garantizar que los esfuerzos de desarrollo de capacidades en este espacio refuercen

los objetivos más amplios de reforzar la integridad de la información y mejorar la confianza de los ciudadanos.

Según la encuesta de la OCDE, el 90 % de los países encuestados indicó que es una prioridad para el futuro desarrollar la capacidad de los funcionarios públicos para rastrear y responder a las amenazas de la desinformación. Sin embargo, solo el 65 % informó haber recibido una formación regular y especializada en la lucha contra la desinformación. Por ejemplo, en Colombia, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) ha adoptado medidas proactivas para formar a su equipo de la Oficina de Prensa. Aquellos que se incorporan al equipo de la Oficina de Prensa reciben capacitación sobre cómo identificar posibles narrativas de desinformación y reaccionar mejor ante estas situaciones. Por su parte, el Ministerio de Asuntos de Interior y Relaciones con el Reino de los Países Bajos redactó en 2022 una «Guía para combatir la desinformación» con el fin de proporcionar a los funcionarios una orientación general (véase Recuadro 4.17).

Recuadro 4.17. Guía para combatir la desinformación – Países Bajos

En enero de 2022, el Ministerio del Interior y Relaciones con el Reino de los Países Bajos elaboró una «Guía para combatir la desinformación», que ofrece a los funcionarios públicos una visión general de cómo se puede difundir y reconocer la información falsa y engañosa; la mecánica de la polarización en el espacio de la información; y asesoramiento jurídico y práctico sobre cómo minimizar el impacto de la desinformación y lo que pueden hacer para combatirla. La guía se estructura en torno a cuatro temas principales:

1. Descripción general de los riesgos y los efectos de la desinformación: Esta sección reitera la importancia de las habilidades de alfabetización mediática e informacional para verificar las fuentes y los contenidos. Asimismo, proporciona una visión general de los riesgos sociales de la desinformación, incluyendo que el contenido deliberadamente falso y engañoso puede exacerbar la polarización y socavar la confianza en la democracia.
2. Preparación: Esta sección presenta una visión general de la importancia de establecer estructuras organizativas eficaces; comunicarse con los medios y el público para desarrollar la alfabetización mediática e informacional; y establecer iniciativas de comunicación pública eficaces y proactivas.
3. Respuesta a la desinformación: Esta sección presenta una descripción general de cómo los comunicadores deben decidir cuál es la mejor manera o incluso si deben responder a narrativas particulares, así como ejemplos de mensajes eficaces.
4. Opciones legales: Esta sección reitera que el gobierno siempre debe actuar dentro del marco constitucional de la libertad de expresión y que el contenido de desinformación no puede simplemente restringirse. Asimismo, establece el marco legal que informa sobre el contenido ilegal y los daños causados por la difusión de contenidos falsos o engañosos.

Fuente: Jahangir (2023[34]), *Disinformation Landscape in the Netherlands*, https://www.disinfo.eu/wp-content/uploads/2023/09/20230919_NL_DisinfoFS.pdf; Ministerio del Interior y Relaciones con el Reino (2022[35]), Handreiking omgaan met desinformatie, https://www.weerbaarbestuur.nl/sites/default/files/inline-files/BZK%20-%20Handreiking%20omgaan%20met%20desinformatie.pdf.

Otro ejemplo es el manual RESIST 2 del Reino Unido, que se utiliza en las formaciones para ayudar a los funcionarios públicos a construir resiliencia individual y social frente a la desinformación a través de la comunicación estratégica (Recuadro 4.18).

Recuadro 4.18. El manual de protección contra la desinformación RESIST del Reino Unido

En 2018, el gobierno del Reino Unido, en consulta con la sociedad civil y los países socios, creó el marco RESIST, un enfoque paso a paso para contrarrestar la desinformación, que ayuda a enfrentarse a este desafío de forma sistemática y eficaz, garantizando al mismo tiempo la protección de los principios democráticos fundamentales como la libertad de expresión. RESIST es el acrónimo de reconocer la información errónea y la desinformación, alerta temprana, conocimiento de la situación, análisis de impacto, comunicación estratégica y eficacia del seguimiento.

Este marco se materializó en un manual público destinado a dar confianza a los comunicadores profesionales y a los ciudadanos a la hora de evaluar la veracidad de la información. Desde la publicación de RESIST en 2019, el gobierno del Reino Unido ha formado a más de quinientos comunicadores de por lo menos 20 países socios mediante una combinación de formaciones presenciales, sesiones remotas y aprendizaje digital.

Desde el marco original RESIST, los profesionales de la comunicación y los funcionarios públicos del Reino Unido y de todo el mundo han proporcionado información sobre cómo utilizan el manual y qué les gustaría ver en futuras versiones. Es por ello que, en 2021, el gobierno del Reino Unido publicó el Manual de protección contra la desinformación RESIST 2, una versión actualizada que refleja tanto las demandas cambiantes de la profesión de la comunicación como el entorno de información en evolución que explora nuevas técnicas y tácticas.

Fuente: Servicio de Comunicación del Gobierno del Reino Unido (2021[36]), RESIST 2 Counter Disinformation Toolkit, https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/.

Los programas de desarrollo de capacidades también deben estar estrechamente vinculados a las últimas investigaciones disponibles. Por lo tanto, la asociación con organizaciones activas en el campo de la integridad de la información puede ayudar a garantizar la provisión de oportunidades de aprendizaje de alta calidad, innovadoras y rentables. Así, los funcionarios públicos de Italia, por ejemplo, se benefician de las formaciones basadas en la investigación del Observatorio Europeo de Medios Digitales, un centro de especialización independiente, que promueve el conocimiento científico sobre la desinformación en línea, fomenta el desarrollo de servicios de verificación de datos y apoya proyectos de alfabetización mediática (véase, Recuadro 4.19 – Puede consultar información adicional sobre la participación con socios no gubernamentales en el Capítulo III).

Recuadro 4.19. Formación del Ministerio de Asuntos Exteriores sobre desinformación y comunicación estratégica – Italia

El Ministerio de Asuntos Exteriores italiano (MFA) proporciona formaciones sobre desinformación y comunicación estratégica como parte de sus esfuerzos de desarrollo de capacidades para diplomáticos, funcionarios públicos en Institutos Culturales Italianos y el personal militar que se va a desplegar en el extranjero. El MFA también apoyó la creación de un centro nacional italiano para combatir la desinformación: el Observatorio Italiano de Medios Digitales (IDMO), un proyecto financiado por la UE, que promueve el conocimiento científico sobre la desinformación en línea, fomenta el desarrollo de servicios de verificación de hechos y apoya los programas de alfabetización mediática. El IDMO trabaja con representantes de embajadas e interlocutores clave como la RAI, la Escuela de Periodismo LUISS y Newsguard, entre otros.

El Ministerio de Asuntos Exteriores italiano también elabora productos de comunicación y coordina campañas en las redes sociales para crear conciencia pública sobre la desinformación, como un episodio especial del podcast «Voci dalla Farnesina» (Voces de la Farnesina), que contó con la participación de periodistas,

académicos y diplomáticos para discutir las diferencias en la terminología entre la información errónea, la desinformación y la información maliciosa, y para alentar a los ciudadanos a pensar críticamente sobre la industria de la manipulación de la información en las plataformas digitales.

Fuente: Observatorio Italiano de Medios Digitales (n.d.[37]), "Uniti contro la disinformazione", https://www.idmo.it/.

Canadá también ha invertido en la formación de funcionarios públicos, centrada en cultivar la comprensión y la resistencia a la desinformación mediante la adaptación del manual RESIST 2 del Reino Unido al contexto canadiense (Recuadro 4.20).

Recuadro 4.20. Formación contra la desinformación de la Oficina del Consejo Privado – Canadá

Canadá ha abordado el fomento de la comprensión y la resiliencia frente a la desinformación en el contexto canadiense mediante la promoción de una ciudadanía informada y comprometida, incluidos sus funcionarios públicos. Con un presupuesto anual de 2 millones de dólares canadienses, la Unidad de Protección de la Democracia de la Oficina del Consejo Privado coordina, desarrolla y aplica medidas gubernamentales para combatir la desinformación. Esto incluye la Lucha contra la desinformación:Una guía para funcionarios públicos, que ofrece orientación sobre cómo sortear la amenaza de la desinformación y la desinformación sobre la base del manual RESIST del Reino Unido. La Escuela de Servicio Público de Canadá también combina la formación presencial a través de cursos híbridos, que abarcan temas como la investigación sobre los impulsores conductuales de la desinformación y la confianza en las instituciones, y el uso de plataformas de redes sociales para la comunicación pública.

Fuente: Gobierno de Canadá (2022[38]), "Backgrounder: Government of Canada to fund projects addressing the growing problem of online mis/disinformation", https://www.canada.ca/en/canadian-heritage/news/2022/07/backgroundergovernment-of-canada-to-fund-projects-addressing-the-growing-problem-of-online-misdisinformation.html; Gobierno de Canadá (n.d.[39]), "Countering Disinformation: A Guidebook for Public Servants", https://www.canada.ca/en/democratic-institutions/services/protecting-democratic-institutions/countering-disinformation-guidebook-public-servants.html; Gobierno de Canadá (2023[40]), "The Trust Series: Trust and Misinformation in Digital Information Ecosystems (TRN1-E11)", https://catalogue.csps-efpc.gc.ca/product?catalog=TRN1-E11&cm_locale=en; Gobierno de Canadá (2022[41]), "Navigating Social Media as a Public Servant (TRN125)", https://catalogue.csps-efpc.gc.ca/product?catalog=TRN125&cm_locale=en.

Las experiencias de los países en materia de desarrollo de capacidades sobre este tema apuntan a la importancia de desarrollar el conocimiento y las competencias de los funcionarios públicos para saber rastrear y contrarrestar la desinformación. Los ejemplos de iniciativas de desarrollo de capacidades apuntan al valor de diseñar programas accesibles y basados en hechos, que tengan en cuenta las sensibilidades culturales y lingüísticas, y que se impartan en diversos formatos, como fuera de línea y en línea, talleres, conjuntos de herramientas y manuales. La experiencia también apunta al valor de fomentar la movilidad personal entre agencias y oficinas para que aprovechen la experiencia entre proyectos y compañeros.

4.4. LOS GOBIERNOS DEBERÁN SEGUIR DESARROLLANDO UNA GOBERNANZA REGULATORIA ÁGIL PARA CONSTRUIR LA INTEGRIDAD DE LA INFORMACIÓN

La regulación es una herramienta esencial para que los gobiernos construyan la integridad de la información, respondan a las amenaza que plantea la desinformación y logren los objetivos sociales de reforzar la democracia en general. Sin embargo, aún quedan preguntas clave sobre qué estrategias seguir y cómo se debería abordar la regulación. Las consideraciones incluyen los procesos y las instituciones que se ponen en marcha para diseñar, aplicar y revisar la regulación (OECD, 2018[42]). Esto también se refleja en la Recomendación del Consejo de la OCDE sobre Gobernanza Regulatoria Ágil (OECD, 2021[43]).

Más recientemente, la OCDE lanzó la iniciativa *Better Regulation in the Digital aGE (BRIDGE)*, con el objetivo de apoyar a los países en la implementación de una gobernanza regulatoria eficaz para las actividades digitales. Cuando se aborda desde la perspectiva de la «mejor regulación», se pone de manifiesto cómo la regulación tiene el poder de gestionar eficazmente los riesgos asociados a las tecnologías digitales, a la vez que promueve la innovación digital. Sin embargo, el ritmo al que se producen los cambios tecnológicos, los regímenes existentes que carecen de agilidad en el mundo digital, las nuevas actividades y modelos de negocio, y la naturaleza global de las actividades digitales están limitando la capacidad de los gobiernos para reforzar eficazmente la integridad de la información.

De cara al futuro, las consideraciones relacionadas con la política regulatoria deberán centrarse, según corresponda, en:

- Fomentar un enfoque de gobernanza regulatoria más ágil para la regulación en el espacio de la información
- Aclarar los enfoques de aplicación de la normativa relacionada con la integridad de la información.

4.4.1. Fomentar un enfoque de gobernanza regulatoria más ágil para la regulación en el espacio de la información

Especialmente en el espacio de la información, que cambia a gran velocidad, la política regulatoria debería diseñarse para ser ágil y responder a los desafíos que plantean la digitalización y las tecnologías emergentes. Mientras que la regulación tradicional suele diseñarse por tema, por sector o por tecnología, las tecnologías de la comunicación digitales y emergentes suelen erosionar, solapar o difuminar las delimitaciones habituales. Las tecnologías digitales y emergentes también desdibujan la distinción tradicional entre consumidores y productores (Amaral et al., 2020[44]).

Así pues, la noción tradicional de responsabilidad suele ser insuficiente a la hora de responder a la desinformación y la información errónea, dado que los riesgos para los afectados, las tecnologías utilizadas y el origen de dichos contenidos pueden encontrarse en jurisdicciones diferentes. La erosión de la delimitación habitual de los mercados socava la pertinencia de los mandatos y las competencias tradicionales de los reguladores. Además, las nuevas formas de comunicación y participación plantean desafíos a la aplicación de las normas existentes; los enfoques fragmentados entre las jurisdicciones impiden enfoques coherentes y coordinados a pesar de los efectos transfronterizos de muchas tecnologías de la información y la comunicación; y el desajuste entre el ritmo del desarrollo tecnológico y el ritmo de evolución de los marcos regulatorios (el «problema del ritmo») plantea nuevos y complejos problemas para los gobiernos y los reguladores (Amaral et al., 2020[44]).

Dados los desafíos regulatorios que plantea la complejidad del espacio de la información, será esencial emprender un cambio en los procesos de política regulatoria. Tal y como señala la Recomendación de la OCDE sobre gobernanza regulatoria ágil para aprovechar la innovación, «la mentalidad tradicional de "regular y olvidar" debería dar paso a los enfoques de "adaptar y aprender". Un enfoque más ágil de la formulación de políticas regulatorias contribuirá a garantizar que los gobiernos tengan la capacidad de comprender las innovaciones y su potencial impacto en las normativas vigentes y en los valores públicos en general (OECD, 2021[45]). En el espacio de la información, la agilidad regulatoria debería dirigirse a comprender los efectos previstos (y no deseados) de las normativas existentes, así como a aplicar las lecciones a las nuevas tecnologías, como la IA generativa.

En este sentido, será importante utilizar herramientas de gestión adecuadas para diseñar, aplicar y evaluar eficazmente las regulaciones. Por ejemplo, establecer mecanismos para la participación del público y de las partes interesadas en el proceso regulador desde una fase temprana y a lo largo de todo el ciclo de políticas podría contribuir a mejorar la transparencia, generar confianza y aprovechar diversas fuentes de experiencia. La realización de evaluaciones de impacto regulatorio (RIA) que evalúen todas las opciones de políticas relevantes, incluidas las alternativas no regulatorias, también es crucial, al igual que la implementación de procesos integrales de RIA y el esbozo de la evaluación posterior (véase Recuadro 4.21 para una descripción general del Informe de evaluación de impacto de la DSA). Finalmente, el monitoreo del impacto de las regulaciones de una manera sistemática y continua, la participación en una reevaluación oportuna y proporcionada y la incorporación de los requisitos de revisión en los marcos apropiados contribuirán al logro de una regulación ágil (OECD, 2021[45]).

Recuadro 4.21. Informe de evaluación de impacto del Reglamento de servicios digitales de la UE

El Informe de evaluación de impacto de la DSA señala que la regulación se fundamenta en la evaluación de la Directiva sobre comercio electrónico de 2000 y que pretende responder a tres problemas centrales, que impulsan la regulación, como son: la exposición de los ciudadanos a cada vez más riesgos en línea, especialmente en las plataformas en línea muy grandes; la supervisión de las plataformas en línea en gran medida descoordinada e ineficaz en la Unión Europea; y el riesgo de que las regulaciones a nivel nacional creen cada vez más barreras en el mercado interior y refuercen las ventajas competitivas de las plataformas muy grandes y de los servicios digitales establecidos.

El Informe de evaluación de impacto también señaló que los beneficios previstos de la DSA serían impulsar la competitividad, la innovación y la inversión en servicios digitales, al tiempo que se abordan los daños específicos. Además, la regulación tratará de promover la transparencia y la seguridad en línea, así como proteger los derechos fundamentales. Una mayor cooperación entre los Estados miembros y la gobernanza a nivel de la UE mejorará la aplicación, logrando así un sistema de supervisión actualizado para los servicios digitales. En particular, el Informe de evaluación de impacto también señala que la revisión debería realizarse en un plazo de cinco años a partir de la entrada en vigor y que los informes periódicos serían parte del diseño del sistema de supervisión.

Fuente: Comisión Europea, Bruselas, 15.12.2020 SWD(2020) 349 final, Resumen del Informe de la Evaluación de Impacto que acompaña al documento: 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.

Dicho esto, abordar el rápido ritmo del progreso tecnológico exige acortar los plazos en todo el proceso de formulación de políticas y utilizar las herramientas de gestión regulatoria de una forma más dinámica. Para contribuir a promover una regulación más ágil y flexible, estos procesos políticos (participación pública, realización de evaluaciones de impacto regulatorio (EIR), seguimiento y evaluación *a posteriori*) no deben acometerse como una serie de requisitos discretos, que se llevan a cabo de forma sucesiva, sino más bien como herramientas complementarias integradas en el ciclo de políticas para informar sobre la adaptación adecuada de los enfoques regulatorios (o alternativos) (OECD, 2021[45])». Garantizar la flexibilidad y la proporcionalidad de la regulación debería estar respaldado por instituciones gubernamentales, que protejan los derechos de las partes interesadas y les proporcionen acceso a mecanismos de indemnización si se vulneran estos derechos (OECD, 2018[46]).

El ritmo y la amplitud del cambio también requieren un enfoque regulatorio más anticipatorio basado en la capacidad institucional y en mecanismos para comprender mejor cómo las tecnologías emergentes pueden afectar a las sociedades, los mercados y las acciones gubernamentales. Cabe destacar que este esfuerzo requerirá el establecimiento de asociaciones constructivas con socios no gubernamentales para facilitar una mayor comprensión -y respuestas más eficaces- a los desafíos que el desarrollo tecnológico plantea a la integridad de la información (OECD, 2022[47]). Los gobiernos también deberían aumentar la capacidad de los organismos de supervisión y de asesoría para prever e implementar una previsión estratégica que oriente el diseño, la implementación y el análisis de las normativas. La creación de capacidades exige dedicar los recursos adecuados a desarrollar las habilidades necesarias para realizar evaluaciones de impacto, construir una prospectiva estratégica y comprender los costes y los beneficios de la innovación y de las nuevas tecnologías (OECD, 2021[43]).

La experimentación, incluso en forma de «sandboxes» regulatorios, puede ayudar a que los marcos sean más adaptables mediante el aprendizaje y el ajuste continuos. También puede contribuir a reducir los niveles de incertidumbre en torno a la toma de decisiones, especialmente en situaciones, en las que no se puede obtener suficiente información fiable sobre los los posibles impactos o la eficacia de las opciones regulatorias mediante enfoques tradicionales, como la recopilación de información y las consultas. Del mismo

modo, puede servir para mejorar la base de evidencia, que puede ayudar a informar la revisión de la normativa existente o inspirar nuevas reglas.

Por último, para garantizar la eficacia, la coherencia y la vigencia de las políticas y marcos regulatorios, especialmente, en un mundo cada vez más interconectado, resulta fundamental la cooperación entre los gobiernos y los responsables políticos de distintas jurisdicciones. En este sentido, la cooperación internacional en materia regulatoria (IRC) es esencial para evitar la fragmentación y prevenir el arbitraje regulatorio, es decir, la práctica de aprovechar las diferencias entre sistemas para eludir normativas más exigentes (OECD, 2012[48]). Además, teniendo en cuenta las importantes necesidades de recursos para regular el espacio de la información, la IRC puede ayudar a los gobiernos y organismos reguladores a orientar y utilizar esos recursos de la forma más eficiente posible.

4.4.2. La aplicación y el cumplimiento de las medidas de regulación requieren objetivos y procesos claros

Las regulaciones en este espacio no pueden lograr sus objetivos establecidos, a menos que los actores cumplan y los requisitos se apliquen adecuadamente. Por ello, los países deberían considerar la implementación de diversas estrategias y mecanismos para garantizar el cumplimiento, incluida una combinación de acciones de seguimiento por parte de órganos de supervisión, seguimiento por parte de auditores externos, así como la previsión y aplicación de sanciones. La integración de estas consideraciones relacionadas con la aplicación en las propuestas legislativas y las evaluaciones relacionadas puede ayudar a proporcionar claridad y dirección.

Estas consideraciones incluyen los requisitos de datos e información para verificar el cumplimiento, así como iniciativas de cooperación institucional y transfronteriza integradas en el uso de herramientas de gestión regulatoria (OECD, 2021[45]). Por ejemplo, la Reglamento de servicios digitales (DSA) exige a las plataformas en línea muy grandes (VLOP) y a los motores de búsqueda en línea muy grandes (VLOBE) que «evalúen los riesgos sistémicos derivados del diseño, el funcionamiento y el uso de sus servicios, así como de los posibles usos indebidos por parte de los destinatarios del servicio, y adopten medidas correctoras adecuadas respetando los derechos fundamentales», y proporcionadas en sus medidas correctoras (DSA, Rec. 79 y Art. 34) (European Union, 2022[49]). Cabe destacar que el Reglamento de servicios digitales (DSA) también requiere que los VLOP y los VLOSE realicen una auditoría independiente de su cumplimiento de las obligaciones de la DSA, incluidos los códigos de conducta y los protocolos de crisis (European Union, 2022[49]). En el futuro, será necesario desarrollar líneas de base para las comparaciones, así como aclarar las distinciones entre los tipos de auditorías (como las evaluaciones de impacto de los algoritmos, las evaluaciones de impacto del sesgo y el etiquetado preciso de los sistemas algorítmicos) para garantizar la coherencia en todo el sector (Singh and Doty, 2021[50]). Los gobiernos podrían facilitar la comparabilidad de las auditorías y las actividades de mitigación de riesgos de las plataformas mediante el desarrollo de pruebas, normas y procesos específicos y cuantificables. (Forum on Information and Democracy, 2020[51]).

Más allá de las acciones y herramientas, los gobiernos también deben identificar qué instituciones se encargarán de aplicar las regulaciones. Dado el papel fundamental que desempeña la información en la democracia y las posibles repercusiones en la libertad de expresión, garantizar que los organismos reguladores sean independientes del gobierno y de aquellos a los que regulan podría generar una mayor confianza en la imparcialidad y justicia de las decisiones (OECD, 2012[48]). Además, la gama de estrategias regulatorias implicadas en el refuerzo de la integridad de la información en los sectores de los medios de comunicación y las comunicaciones pone de manifiesto la dificultad de identificar a los actores adecuados para aplicar las regulaciones. El creciente papel y el impacto de los contenidos digitales hacen que las autoridades, incluidas las de protección de datos y privacidad, competencia, medios de comunicación, protección del consumidor, telecomunicaciones, elecciones y otras, puedan desempeñar un papel en la aplicación de la normativa en este ámbito.

Por su parte, el Reglamento europeo de servicios digitales (DSA) permite flexibilidad a este respecto. Por un lado, debido a la «naturaleza transfronteriza de los servicios en cuestión y al alcance horizontal de las obligaciones (de la DSA)», la ley exige a los Estados miembros que designen un Coordinador de Servicios Digitales para que «actúe como único punto de contacto en todos los asuntos relacionados con la aplicación de este reglamento (European Union,

2022[49])». Sin embargo, el Reglamento europeo de servicios digitales (DSA) también señala que los Estados miembros pueden recurrir a más de una autoridad y, en particular, a una con conocimientos específicos o competencias ejecutivas (como los reguladores de las comunicaciones electrónicas, los reguladores de los medios de comunicación o las autoridades de protección del consumidor), para apoyar la aplicación de la legislación (European Union, 2022[49]).

4.5. CONSIDERACIONES Y EL CAMINO A SEGUIR

Los gobiernos han reconocido cada vez más la necesidad de establecer procesos y estructuras de gobernanza responsables, transparentes y ágiles, a medida que buscan desarrollar respuestas eficaces para las amenazas que supone la desinformación y reforzar la integridad de la información. La eficacia de las respuestas de gobernanza dentro de las democracias no solo se limita a contrarrestar la desinformación. En un sentido más amplio, la eficacia se refiere a unos ecosistemas de información libres, diversos y transparentes, que crean las condiciones necesarias para que los ciudadanos tomen decisiones bien fundamentadas y participen en un diálogo cívico constructivo, todo ello protegiendo los derechos humanos de todos. Estos esfuerzos serán más efectivos si se centran en la diversidad y la inclusión desde la base, abarcando aspectos tales como la dotación de personal, la planificación estratégica y las asociaciones. Esto permitirá incorporar a personas con las competencias y experiencias adecuadas para abordar algunos de los temas más acuciantes en materia de integridad de la información.

Para ello, los gobiernos deberán adaptar y mejorar su arquitectura institucional persiguiendo los siguientes objetivos, según corresponda:

- Desarrollar e implementar marcos estratégicos que respalden una visión coherente y un enfoque integral para reforzar la integridad de la información. Esta orientación puede articularse mediante estrategias nacionales centradas específicamente en la desinformación y en la integridad de la información, o bien incluida como parte de otros documentos oficiales, tales como las estrategias nacionales de defensa y de seguridad, digitalización, comunicaciones públicas, cultura y educación. Unos marcos estratégicos eficaces describen los objetivos, los plazos y el alcance de la acción, así como los aspectos operativos relativos al entorno institucional, los informes y los procesos de evaluación. Un análisis más detallado permitirá identificar tendencias y mejores prácticas para mejorar el papel de la orientación estratégica en este ámbito.
- Crear oficinas, unidades o mecanismos de coordinación claramente definidos para promover acciones de apoyo mutuo entre los organismos gubernamentales encargados de abordar las amenazas de la desinformación y reforzar la integridad de la información. Un enfoque interinstitucional bien coordinado podría ayudar a los países a establecer conexiones con las prioridades sectoriales, favorecer el intercambio rápido de información y evitar la duplicación de esfuerzos entre las autoridades institucionales. Los gobiernos también podrían considerar la creación de grupos de trabajo para proporcionar asesoramiento experto sobre políticas relacionadas con las dimensiones técnicas de la desinformación tales como las amenazas híbridas, la interferencia extranjera y la interferencia electoral. Un enfoque multinstitucional también ayudará a alinear las necesidades a corto plazo, como el suministro de información relacionada con crisis, elecciones o amenazas inmediatas, con objetivos a más largo plazo relacionados con la construcción de la integridad de la información y la resiliencia social. Priorizar la creación de mecanismos para garantizar una comunicación eficaz, así como el intercambio de información y la construcción de relaciones entre el personal dentro de las entidades y entre ellas. Favorecer una cultura basada en los hechos, que incorpore la medición y evaluación de cada etapa del proceso de desarrollo e implementación de las políticas.
- Describir el funcionamiento y los objetivos de las oficinas y unidades pertinentes en las disposiciones legales que definen el mandato y los parámetros dentro de los cuales operan. Estas disposiciones son importantes para establecer procedimientos de rendición de cuentas y de presentación de informes, así

como para ayudar a garantizar que las actividades gubernamentales no infrinjan los derechos ni las libertades fundamentales.

- Mejorar la cooperación internacional para fortalecer la respuesta democrática a los desafíos en el espacio de la información mediante asociaciones y alianzas, y conectando y habilitando las redes existentes en los diferentes sectores. El intercambio de inteligencia estratégica y de metodologías analíticas, así como las respuestas políticas y sus resultados podría ayudar a aprovechar las enseñanzas relevantes e identificar las mejores prácticas.
- Ofrecer oportunidades de desarrollo de capacidades a nivel local, nacional e internacional para los funcionarios públicos que se enfrentan a los retos correspondientes en su trabajo diario. El nivel de sofisticación de las campañas de desinformación requiere emprender una labor de formación y cualificación en todos los niveles de gobierno, para garantizar que los administradores públicos y los responsables políticos posean los conocimientos y las herramientas necesarios para reconocer, monitorear y contrarrestar la difusión de información falsa y engañosa sin constreñir la libertad de expresión. Promover la diversidad en las plantillas de personal y la cultura de la inclusión; estos principios no solo son valores democráticos fundamentales, sino también una piedra angular necesaria para disponer de unas medidas eficaces contra la desinformación y su impacto, gracias a la naturaleza multidisciplinaria del problema y de las soluciones.
- Implementar respuestas normativas ágiles a los desafíos que plantean las tecnologías de comunicación emergentes. Especialmente en el espacio de la información, caracterizado por unas novedosas formas de comunicación que difuminan las delimitaciones tradicionales entre los sectores regulados, la política normativa debería adaptarse y aprender a lo largo de todo el ciclo, incluida una mejor coordinación entre las autoridades para reducir las respuestas fragmentadas del gobierno. Los gobiernos deberán establecer mecanismos para la participación del público y de las partes interesadas en el proceso regulatorio; aplicar procesos exhaustivos de evaluación del impacto de la normativa (EIAN); realizar evaluaciones y seguimientos del impacto; así como, evaluar los mecanismos y autoridades de auditoría y aplicación adecuados;
- Aumentar la capacidad de los organismos de supervisión y de asesoría normativa para prever la evaluación del ecosistema de información e implementar una previsión estratégica que oriente el diseño, la implementación y el análisis de las normativas. La mejora de la capacidad y la flexibilidad de las entidades reguladoras también facilitará la experimentación, incluso en forma de «sandboxes» o espacios controlados de pruebas, de modo que los marcos resultantes sean más adaptables.
- Reforzar la cooperación internacional en materia de regulación para evitar la fragmentación y prevenir el arbitraje regulatorio. Dada la naturaleza intrínsecamente global de los flujos de información en línea, es esencial la cooperación entre los gobiernos y responsables políticos para garantizar la eficacia, la eficiencia, la coherencia y la vigencia de las políticas y marcos regulatorios.

4.6. NOTA METODOLÓGICA

El capítulo presenta un análisis basado en la evidencia del mecanismo de coordinación relevante y las prioridades estratégicas establecidas a nivel nacional para abordar la difusión de información falsa y engañosa. Este capítulo incluye datos de 24 países miembros de la OCDE obtenidos de la encuesta «Arquitectura institucional y prácticas de gobernanza para fortalecer la integridad de la información», diseñada por el equipo del Centro de Recursos DIS/MIS de la OCDE. Los países participantes son Alemania, Canadá, Chile, Colombia, Costa Rica, Estonia, Finlandia, Francia, Grecia, Italia, Irlanda, Letonia, Lituania, Luxemburgo, Países Bajos, Noruega, Portugal, República Eslovaca, España, Suecia, Suiza, Turquía y Estados Unidos. Las respuestas fueron proporcionadas por las autoridades gubernamentales entre abril y septiembre de 2023. Dado el rápido ritmo de los avances en el campo de la desinformación y la integridad de la información, es importante tener en cuenta que este capítulo refleja la situación existente en septiembre de 2023.

REFERENCIAS

Amaral, M. et al. (2020), *Principles on effective and innovation-friendly rulemaking in the Fourth Industrial Revolution – Background paper*. [44]

Butcher, P. (2019), "Disinformation and democracy: The home front in the information war", *EPC Discussion Paper*. [7]

European Union (2022), *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*, Publications Office of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?ur. [49]

European Union External Action Service (2023), *1st EEAS Report on Foreign Information Manipulation and Interference Threats*. [1]

Federal Ministry of the Interior and Community (2023), *Measures taken by the Federal Government to fight disinformation*, https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation/measures-taken-by-the-federal-government.html. [16]

Forum on Information & Democracy (n.d.), "International Partnership for Information & Democracy", https://informationdemocracy.org/international-partnership-on-information-democracy/ (accessed on 15 February 2024). [32]

Forum on Information and Democracy (2023), *Pluralism of news and information in curation and indexing algorithms*, https://informationdemocracy.org/wp-content/uploads/2023/08/Report-on-Pluralism-Forum-on-ID.pdf. [31]

Forum on Information and Democracy (2020), *Working Group on Infodemics: Policy Framework*, https://informationdemocracy.org/wp-content/uploads/2020/11/ForumID_Report-on-infodemics_101120.pdf. [51]

Government of Brazil (2023), *Institution of the Committee to Combat Disinformation on the National Program of Immunizations and Public Health Policies*, Presidency of the Presidency of the Republic, https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11753.htm. [18]

Government of Canada (2023), "The Trust Series: Trust and Misinformation in Digital Information Ecosystems (TRN1-E11)", https://catalogue.csps-efpc.gc.ca/product?catalog=TRN1-E11&cm_locale=en. [40]

Government of Canada (2022), "Backgrounder: Government of Canada to fund projects addressing the growing problem of online mis/disinformation", https://www.canada.ca/en/canadian-heritage/news/2022/07/backgroundergovernment-of-canada-to-fund-projects-addressing-the-growing-problem-of-online-misdisinformation.html. [38]

Government of Canada (2022), "Navigating Social Media as a Public Servant (TRN125)", https://catalogue.csps-efpc.gc.ca/product?catalog=TRN125&cm_locale=en. [41]

Government of Canada (n.d.), "Countering Disinformation: A Guidebook for Public Servants", https://www.canada.ca/en/democratic-institutions/services/protecting-democratic-institutions/countering-disinformation-guidebook-public-servants.html (accessed on 15 February 2024). [39]

Government of Ireland (2023), *National Counter Disinformation Strategy Working Group*, https://www.gov.ie/en/publication/04f9e-national-counter-disinformation-strategy-working-group/#. [5]

Government of the Netherlands (2023), *Global Declaration on Information Integrity Online*, https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2023/09/20/global-declaration-on-information-integrity-online. [28]

Government of the Netherlands (2023), *Global Declaration on Information Integrity Online*, Ministry of Foreign Affairs, https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2023/09/20/global-declaration-on-information-integrity-online. [29]

Government of the Netherlands (2022), *Government-wide strategy for effectively tackling disinformation*, Ministry of the Interior and Kingdom Relations, https://www.government.nl/documents/parliamentary-documents/2022/12/23/government-wide-strategy-for-effectively-tackling-disinformation. [3]

Government of the Republic of Lithuania (2023), "Lithuania's new crisis management model presented at Baltic States Centres of Government Meeting", The Office of the Government of the Republic of Lithuania, https://lrv.lt/en/news/lithuanias-new-crisis-management-model-presented-at-baltic-states-centres-of-government-meeting/. [10]

Government of the Slovak Republic (2023), *The concept of strategic communication of the Slovak Republic*, https://www.vlada.gov.sk/share/uvsr/koncepcia_strategickej%20komunikacie_sr.pdf?csrt=934388656163986176. [4]

Hybrid CoE (n.d.), "What is Hybrid CoE?", The European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/about-us/ (accessed on 19 October 2023). [24]

IDMO (n.d.), "Uniti contro la disinformazione", Italian Digital Media Observatory, https://www.idmo.it/ (accessed on 10 December 2023). [37]

Instytut Kościuszki (2022), *Report – Resilience to Disinformation*, Instytut Kościuszki, https://ik.org.pl/en/publikacje/4850/. [27]

Jahangir, R. (2023), *Disinformation Landscape in the Netherlands*, EU DisinfoLab, https://www.disinfo.eu/wp-content/uploads/2023/09/20230919_NL_DisinfoFS.pdf. [34]

Jeangène Vilmer, J. (2021), *Effective state practices against disinformation: Four country case studies*. [22]

Kleis Nielsen, R. (2021), *How to respond to disinformation while protecting free speech*. [6]

Latvijas Vēstnesis (2023), "Valsts informatīvās telpas drošības koordinācijas grupas nolikums", Ministru kabineta noteikumi Nr. 236, Rīgā 2023. gada 9. maijā (prot. Nr. 25 28. §), https://likumi.lv/ta/id/341811-valsts-informativas-telpas-drosibas-koordinacijas-grupas-nolikums. [8]

Lewandowsky, S. (2021), "Climate Change Disinformation and How to Combat It", *Annual Review of Public Health*, Vol. 42/1, pp. 1-21, https://doi.org/10.1146/annurev-publhealth-090419-102409. [20]

Ministry of Science, Technology, Knowledge and Innovation (n.d.), "Comisión Asesora contra la Desinformación", https://www.minciencia.gob.cl/areas/comision-contra-la-desinformacion/ (accessed on 15 February 2024). [17]

Ministry of the Interior and Kingdom Relations (2022), *Handreiking omgaan met desinformatie*, Ministry of the Interior and Kingdom Relations, https://www.weerbaarbestuur.nl/sites/default/files/inline-files/BZK%20-%20Handreiking%20omgaan%20met%20desinformatie.pdf. [35]

NATO (2023), "Countering hybrid threats", North Atlantic Treaty Organization, https://www.nato.int/cps/en/natohq/topics_156338.htm. [23]

OECD (2023), *Public Communication Scan of the United Kingdom: Using Public Communication to Strengthen Democracy and Public Trust*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/bc4a57b3-en. [15]

OECD (2022), *Building Trust and Reinforcing Democracy: Preparing the Ground for Government Action*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/76972a4a-en. [47]

OECD (2022), *Recommendation of the Council on International Regulatory Co-operation to Tackle Global Challenges*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0475. [33]

OECD (2021), *OECD Report on Public Communication: The Global Context and the Way Forward*, OECD Publishing, Paris, https://doi.org/10.1787/22f8031c-en. [14]

OECD (2021), *Practical Guidance on Agile Regulatory Governance to Harness Innovation*, OECD. [43]

OECD (2021), "Recommendation of the Council for Agile Regulatory Governance to Harness Innovation", OECD/LEGAL/0464, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464. [45]

OECD (2020), *OECD Public Integrity Handbook*, OECD Publishing, Paris, https://doi.org/10.1787/ac8ed8e8-en. [2]

OECD (2018), *Flexibility and Proportionality in Corporate Governance*, OECD Publishing, Paris, https://doi.org/10.1787/9789264307490-en. [46]

OECD (2018), *OECD Regulatory Policy Outlook 2018*, OECD Publishing, Paris, https://doi.org/10.1787/9789264303072-en. [42]

OECD (2012), "Recommendation of the Council on Regulatory Policy and Governance", *OECD Legal Instruments*, OECD/LEGAL/0390, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0390. [48]

Pamment, J. (2020), *The EU's Role in Fighting Disinformation: Taking Back the Initiative*. [19]

SGDSN (2022), *Service de vigilance et protection contre les ingérences numériques étrangères "VIGINUM"*, Secrétariat général de la défense et de la sécurité nationale, https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques. [11]

Singh, S. and L. Doty (2021), *Cracking Open the Black Box: Promoting Fairness, Accountability, and Transparency Around High-Risk AI*, Open Technology Institute, https://www.newamerica.org/oti/reports/cracking-open-the-black-box/. [50]

State Security Department of Lithuania (2022), "Threat Assessments", https://www.vsd.lt/en/threats/threats-national-security-lithuania/. [9]

Swedish Psychological Defence Agency (2023), *Swedish Psychological Defence Agency website*, Psychological Defence Agency, https://www.mpf.se/en/about-us/ (accessed on 31 August 2023). [12]

TTC (2023), *U.S.-EU Joint Statement of the Trade and Technology Council*, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/31/u-s-eu-joint-statement-of-the-trade-and-technology-council-2/. [30]

U.S. Department of State (2024), "The Framework to Counter Foreign State Information Manipulation", https://www.state.gov/the-framework-to-counter-foreign-state-information-manipulation/. [26]

U.S. Department of State (n.d.), "About Us – Global Engagement Center", https://www.state.gov/about-us-global-engagement-center-2/ (accessed on 31 August 2023). [13]

UK Government Communication Service (2021), *RESIST 2 Counter Disinformation Toolkit*, Government Communication Service, https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/. [36]

UNDP (2021), *Information Asymmetries in the Digital Sexual and Reproductive Health Space*. [21]

UNESCO (2023), *Guidelines for Regulating Digital Platforms: Safeguarding freedom of expression and access to information through a multi-stakeholder approach*, United Nations Educational, Scientific and Cultural Organization, https://unesdoc.unesco.org/ark:/48223/pf0000387339. [25]

NOTAS

[1] En la encuesta se preguntaba a los encuestados: *«Para entender mejor sus prioridades en el futuro, indique las áreas en las que su gobierno tratará de mejorar en los próximos 1 a 2 años»*. Una de las prioridades sugeridas fue: Desarrollar, actualizar o aumentar la relevancia de las directrices y/o documentos estratégicos.

[2] En la encuesta se preguntó a los participantes: *¿Existe un marco estratégico nacional o un documento de orientación en vigor, en el que el gobierno identifique y describa las principales amenazas informativas, los posibles impactos y las opciones de respuesta?*

[3] Estrategia Nacional de Ciberseguridad IV https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/strategie-nationale-cybersecurite-4/National-Cybersecurity-Strategy-IV.pdf.

[4] En la encuesta se preguntó a los encuestados "*¿Existe un mecanismo intergubernamental (célula, oficina, unidad, etc.) para coordinar los esfuerzos del gobierno para identificar y/o responder a la desinformación?*".

[6] Para obtener información adicional, consulte: https://www.oecd.org/stories/dis-misinformation-hub/.

[7] Para obtener información adicional, consulte el trabajo del Observatorio de Políticas de Inteligencia Artificial de la OCDE (https://oecd.ai/en/) y de la Secretaría de la Alianza Global sobre Inteligencia Artificial (GPAI) de 29 miembros (https://gpai.ai/), creada en el seno de la OCDE.

[8] Para obtener información adicional, consulte el trabajo de la Red de Gobernanza del Comité de Asistencia para el Desarrollo de la OCDE (GovNet): https://www.oecd.org/dac/accountable-effective-institutions/about-govnet.htm.

[9] Para obtener información adicional, consulte el Marco Voluntario de Informes de Transparencia: https://www.oecd.org/digital/vtrf/.

[10] Para obtener información adicional: https://euvsdisinfo.eu/about/.

[11] Para obtener información adicional, consulte: https://www.unesco.org/en/media-information-literacy.

[12] Para obtener información adicional, consulte: https://www.undp.org/policy-centre/oslo/information-integrity.

[13] Para obtener información adicional, consulte: https://summitfordemocracyresources.eu/about/about-the-summit-for-democracy/.