**Parlamento Europeo**
2019-2024

*Documento de sesión*

**A9-0022/2022**

8.2.2022

# INFORME

sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, en particular la desinformación
(2020/2268(INI))

Comisión Especial sobre Injerencias Extranjeras en Todos los Procesos Democráticos de la Unión Europea, en particular la Desinformación

Ponente: Sandra Kalniete

# ÍNDICE

**Página**

# PROPUESTA DE RESOLUCIÓN DEL PARLAMENTO EUROPEO

**sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, en particular la desinformación**
**(2020/2268(INI))**

*El Parlamento Europeo*,

– Vista la Carta de los Derechos Fundamentales de la Unión Europea, y en particular sus artículos 7, 8, 11, 12, 39, 40, 47 y 52,

– Vista la Carta de las Naciones Unidas, y en particular sus artículos 1 y 2,

– Vista la Resolución 2131 (XX) de la Asamblea General de las Naciones Unidas, de 21 de diciembre de 1965, titulada «Declaración sobre la inadmisibilidad de la intervención en los asuntos internos de los Estados y protección de su independencia y soberanía»,

– Visto el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, y en particular sus artículos 8, 9, 10, 11, 12, 13, 14, 16 y 17, así como el Protocolo de dicho Convenio, y en particular su artículo 3,

– Vistas su Resolución, de 23 de noviembre de 2016, sobre la comunicación estratégica de la Unión para contrarrestar la propaganda de terceros en su contra[1] y su Recomendación, de 13 de marzo de 2019, de hacer balance del seguimiento realizado por el SEAE dos años después del informe del PE sobre la comunicación estratégica de la Unión para contrarrestar la propaganda en su contra por parte de terceros[2],

– Vista su Resolución, de 13 de junio de 2018, sobre ciberdefensa[3],

– Vistas las comunicaciones conjuntas de la Comisión y el alto representante de la Unión para Asuntos Exteriores y Política de Seguridad, de 5 de diciembre de 2018, titulada «Plan de Acción contra la desinformación» (JOIN(2018)0036) y de 14 de junio de 2019, titulada «Informe sobre la ejecución del Plan de acción contra la desinformación» (JOIN(2019)0012),

– Vistos el documento de trabajo conjunto, de 23 de junio de 2021, sobre el quinto informe de situación sobre la ejecución del marco común de 2016 de lucha contra las amenazas híbridas y la Comunicación conjunta de 2018 sobre el aumento de la resiliencia y el desarrollo de las capacidades para hacer frente a las amenazas híbridas (SWD(2021)0729),

– Visto el Plan de Acción para la Democracia Europea (COM(2020)0790),

– Vista la Comunicación de la Comisión, de 3 de diciembre de 2020, titulada «Los medios

[1] DO C 224 de 27.6.2018, p. 58.
[2] DO C 23 de 21.1.2021, p. 152.
[3] DO C 28 de 27.1.2020, p. 57.

de comunicación europeos en la Década Digital: un plan de acción para apoyar la recuperación y la transformación» (COM(2020)0784),

– Visto el paquete de medidas de la Ley de servicios digitales,

– Vista su Resolución, de 20 de octubre de 2021, titulada «Los medios de comunicación europeos en la Década Digital: un plan de acción para apoyar la recuperación y la transformación»[4],

– Vistos el Código de Buenas Prácticas en materia de Desinformación de 2018 y las Orientaciones de 2021 sobre el refuerzo del Código de Buenas Prácticas en materia de Desinformación (COM(2021)0262), así como las Recomendaciones para el nuevo Código de Buenas Prácticas en materia de Desinformación publicadas por el Grupo de Entidades Reguladoras Europeas para los Servicios de Comunicación Audiovisual en octubre de 2021,

– Visto el Informe Especial 09/2021 del Tribunal de Cuentas Europeo titulado «El impacto de la desinformación en la UE: una cuestión abordada, pero no atajada»,

– Vista la propuesta de la Comisión, de 16 de diciembre de 2020, de una Directiva del Parlamento Europeo y del Consejo relativa a la resiliencia de las entidades críticas (COM(2020)0829) y el anexo propuesto a la Directiva,

– Visto el Reglamento (UE) 2019/452 del Parlamento Europeo y del Consejo, de 19 de marzo de 2019, por el que se establece un marco para el control de las inversiones extranjeras directas en la Unión[5] (Reglamento para el control de las IED) y las Orientaciones de marzo de 2020 sobre el Reglamento de control de las IED (C(2020)1981),

– Vista la Comunicación conjunta de la Comisión y el alto representante de la Unión para Asuntos Exteriores y Política de Seguridad, de 16 de diciembre de 2020, titulada «La Estrategia de Ciberseguridad de la UE para la Década Digital» (JOIN(2020)0018),

– Vistos los Artículos de la Comisión de Derecho Internacional sobre la responsabilidad del Estado por hechos internacionalmente ilícitos,

– Vista la propuesta de la Comisión, de 16 de diciembre de 2020, de una Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148 (COM(2020)0823),

– Visto el conjunto de instrumentos de la UE para la seguridad de las redes 5G de marzo de 2021,

– Visto el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad)

[4] Textos Aprobados, P9_TA(2021)0428.
[5] DO L 79 I de 21.3.2019 p. 1.

y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013[6],

– Vistos los estudios, briefings y análisis en profundidad pedidos por la Comisión Especial sobre Injerencias Extranjeras en Todos los Procesos Democráticos de la Unión Europea, en particular la Desinformación (INGE),
– Vista la audiencia de Frances Haugen, de 8 de noviembre de 2021, organizada por su Comisión de Mercado Interior y Protección del Consumidor, en asociación con otras comisiones,

– Vista su Resolución, de 7 de octubre de 2021, sobre la situación de las capacidades de ciberdefensa de la UE[7],

– Vistos los Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas, en particular el ODS 16, que busca promover sociedades pacíficas e inclusivas en favor del desarrollo sostenible,

– Vistos el discurso y la carta de intenciones sobre el estado de la Unión 2021,

– Visto el Informe del secretario general de las Naciones Unidas, de 10 de septiembre de 2021, titulado «Nuestra agenda común»,

– Vista la Comunicación conjunta de la Comisión y del alto representante de la Unión para Asuntos Exteriores y Política de Seguridad, de 10 de junio de 2020, titulada «La lucha contra la desinformación acerca de la COVID-19: contrastando los datos» (JOIN(2020)0008),

– Vista la Decisión del Consejo, de 15 de noviembre de 2021, de modificar su régimen de sanciones contra Bielorrusia para ampliar los criterios de adopción de medidas a fin de dirigir las sanciones contra personas y entidades que organicen o contribuyan a los ataques híbridos y a la instrumentalización de seres humanos llevados a cabo por el régimen de Bielorrusia,

– Vista su Decisión, de 18 de junio de 2020, sobre la constitución, competencias, composición numérica y duración del mandato de la Comisión Especial sobre Injerencias Extranjeras en Todos los Procesos Democráticos de la Unión Europea, en particular la Desinformación[8], adoptada de conformidad con el artículo 207 de su Reglamento interno,

– Visto el artículo 54 de su Reglamento interno,

– Visto el informe de la Comisión Especial sobre Injerencias Extranjeras en Todos los Procesos Democráticos de la Unión Europea, en particular la Desinformación (A9-0022/2022),

A. Considerando que las injerencias extranjeras constituyen una grave violación de los

[6] DO L 151 de 7.6.2019, p. 15.
[7] Textos Aprobados, P9_TA(2021)0412.
[8] DO C 362 de 8.9.2021, p. 186.

valores y principios universales en los que se fundamenta la Unión, como la dignidad humana, la libertad, la igualdad, la solidaridad, el respeto de los derechos humanos y las libertades fundamentales, la democracia y el Estado de Derecho;

B. Considerando que las injerencias extranjeras, la manipulación de la información y la desinformación constituyen un abuso de las libertades fundamentales de expresión e información establecidas en el artículo 11 de la Carta de los Derechos Fundamentales de la Unión Europea y amenazan tales libertades, así como los procesos democráticos en la Unión y sus Estados miembros, como la celebración de elecciones libres y justas; que el objetivo de las injerencias extranjeras es distorsionar los hechos o presentarlos de manera incorrecta, inflar artificialmente argumentos unilaterales, desacreditar la información para degradar el discurso político y, en última instancia, minar la confianza en el sistema electoral y, por tanto, en el propio proceso democrático;

C. Considerando que toda acción contra las injerencias extranjeras y la manipulación de la información debe respetar a su vez las libertades fundamentales de expresión e información; que la Agencia de los Derechos Fundamentales de la Unión Europea (FRA) desempeña un papel clave en la evaluación del respeto de los derechos fundamentales, incluido el artículo 11 de la Carta de los Derechos Fundamentales, a fin de evitar acciones desproporcionadas; que los agentes que realizan injerencias extranjeras y manipulaciones de información hacen un uso indebido de estas libertades en su beneficio, por lo que es fundamental intensificar la lucha preventiva contra las injerencias extranjeras y la manipulación de la información, ya que la democracia depende de que las personas tomen decisiones con conocimiento de causa;

D. Considerando que las pruebas demuestran que agentes estatales y no estatales extranjeros malintencionados y autoritarios, como Rusia y China, entre otros, utilizan la manipulación de la información y otras tácticas de injerencia para interferir en los procesos democráticos en la Unión; que estos ataques, que forman parte de una estrategia de guerra híbrida y constituyen una violación del Derecho internacional, inducen a error y engañan a los ciudadanos y afectan a su comportamiento electoral, amplifican los debates polémicos, dividen, polarizan y explotan las vulnerabilidades de las sociedades, promueven la incitación al odio, agravan la situación de los grupos vulnerables que tienen más probabilidades de ser víctimas de la desinformación, distorsionan la integridad de las elecciones y referendos democráticos, siembran la desconfianza en los Gobiernos nacionales, las autoridades públicas y el orden democrático liberal y tienen por objeto desestabilizar la democracia europea y, por lo tanto, constituyen una grave amenaza para la seguridad y la soberanía de la Unión;

E. Considerando que las injerencias extranjeras constituyen un patrón de conducta que amenaza o afecta negativamente a valores, procedimientos democráticos, procesos políticos, la seguridad de Estados y ciudadanos y la capacidad de hacer frente a situaciones excepcionales; que dichas injerencias tienen un carácter manipulador y se llevan a cabo y se financian de forma intencionada y coordinada; que los responsables de dichas injerencias, incluidos sus intermediarios dentro y fuera de su propio territorio, pueden ser agentes estatales o no estatales y a menudo reciben la ayuda de cómplices políticos en los Estados miembros que obtienen ventajas políticas y económicas de favorecer estrategias extranjeras; que el empleo por parte de agentes extranjeros de personas interpuestas nacionales y la cooperación con aliados nacionales difuminan la

línea de separación entre la injerencia extranjera y la interna;

F. Considerando que las tácticas de injerencia extranjera adoptan, entre otras, las formas de desinformación, supresión de información, manipulación de plataformas de redes sociales y de sus algoritmos, términos y condiciones y sistemas publicitarios, ciberataques, operaciones de pirateo y filtración, amenazas y acoso para acceder a información sobre los votantes e interferir en la legitimidad del proceso electoral, amenazas y acoso contra periodistas, investigadores, políticos y miembros de organizaciones de la sociedad civil, donaciones y préstamos encubiertos a partidos políticos, campañas que favorecen a determinados candidatos, organizaciones y medios de comunicación, organizaciones y medios de comunicación falsos o interpuestos, captación y cooptación de élites, dinero negro, personalidades e identidades falsas, ejercicio de presiones para procurar la autocensura, explotación abusiva de narrativas históricas, religiosas y culturales, ejercicio de presiones sobre instituciones educativas y culturales, asunción del control de infraestructuras críticas, ejercicio de presiones sobre ciudadanos extranjeros que viven en la Unión, instrumentalización de migrantes y espionaje; que estas tácticas se combinan a menudo para tener un mayor efecto;

G. Considerando que la manipulación de la información y la difusión de desinformación pueden servir a los intereses económicos de agentes estatales y no estatales y sus intermediarios y crear dependencias económicas que pueden explotarse con fines políticos; que, en un mundo de competencia internacional no cinética, la injerencia extranjera puede ser una herramienta primordial para desestabilizar y debilitar a las contrapartes a las que se dirige, o para potenciar la propia ventaja competitiva mediante el establecimiento de canales de influencia, dependencias en la cadena de suministro, chantaje o coacción; que la desinformación está causando daños económicos directos e indirectos que no se han evaluado sistemáticamente;

H. Considerando que la información errónea es una información falsa que puede comprobarse y no tiene la intención de causar daño, mientras que la desinformación es una información falsa o engañosa que puede comprobarse y que se crea, presenta o difunde intencionadamente con el propósito de causar daño o provocar un efecto potencialmente perturbador para la sociedad engañando al público o con la intención de obtener un beneficio económico;

I. Considerando que es necesario llegar a un acuerdo, dentro de la Unión, sobre unas definiciones y metodologías comunes y granulares para mejorar el conocimiento común de las amenazas y elaborar normas adecuadas de la Unión para mejorar la imputación y la respuesta; que el Servicio Europeo de Acción Exterior (SEAE) ha realizado un trabajo considerable en este ámbito; que estas definiciones deben garantizar la impermeabilidad a las injerencias externas y el respeto de los derechos humanos; que es de suma importancia la cooperación con socios afines, en los foros internacionales pertinentes, respecto a unas definiciones comunes en materia de injerencia extranjera, con el fin de establecer normas y estándares internacionales; que la Unión debe tomar la iniciativa en el establecimiento de normas internacionales claras para la imputación de injerencias extranjeras;

***Necesidad de una estrategia coordinada contra la injerencia extranjera***

J. Considerando que los intentos de injerencia extranjera en todo el mundo están aumentando y se están volviendo cada vez más sistémicos y sofisticados, basándose en un uso generalizado de la inteligencia artificial (IA) y erosionando la imputabilidad;

K. Considerando que es obligación de la Unión y de sus Estados miembros defender a todos los ciudadanos e infraestructuras, así como a sus sistemas democráticos, de los intentos de injerencia extranjera; que, sin embargo, la Unión y sus Estados miembros parecen carecer de los medios adecuados y suficientes para prevenir, detectar, imputar y contrarrestar y sancionar mejor estas amenazas;

L. Considerando que muchos responsables políticos, y los ciudadanos en general, no son conscientes en la mayoría de los casos de la realidad de estas cuestiones, lo que puede contribuir involuntariamente a la generación de nuevas vulnerabilidades; que la cuestión de las campañas de desinformación no ha sido prioritaria para los responsables políticos europeos; que las audiencias y el trabajo de la Comisión Especial INGE han contribuido al reconocimiento público y a la contextualización de estas cuestiones y han enmarcado con éxito el debate europeo sobre las injerencias extranjeras; que las prolongadas actividades de desinformación extranjeras ya han contribuido a la aparición de desinformación local propia;

M. Considerando que el seguimiento transparente de la situación de las injerencias extranjeras en tiempo real por parte de organismos institucionales y de verificadores de datos y analistas independientes, la coordinación eficaz de su actuación y el intercambio de información en tiempo real es crucial para que se adopten las medidas apropiadas, no solo con el fin de proporcionar información sobre los ataques malintencionados en curso, sino también de contrarrestarlos; que es necesario prestar una atención similar a la cartografía de la sociedad, a la identificación de sus partes más vulnerables y susceptibles de manipulación y desinformación extranjeras y a la eliminación de las causas de esas vulnerabilidades;

N. Considerando que la primera prioridad de la defensa de la Unión, esto es, la resiliencia y la preparación de los ciudadanos de la Unión frente a la injerencia extranjera y la manipulación de la información, requiere un enfoque a largo plazo y de toda la sociedad, empezando por la educación y la concienciación sobre los problemas en una fase temprana;

O. Considerando que es necesario cooperar y coordinarse por lo que respecta a los niveles y sectores administrativos entre los diferentes Estados miembros, a escala de la Unión y con países afines, así como con la sociedad civil y el sector privado, para identificar vulnerabilidades, detectar ataques y neutralizarlos; que existe una necesidad urgente de sincronizar la percepción de las amenazas con la seguridad nacional;

***Refuerzo de la resiliencia mediante la conciencia situacional, la alfabetización mediática e informativa, el pluralismo de los medios de comunicación, el periodismo independiente y la educación***

P. Considerando que la conciencia situacional, unos sistemas democráticos sólidos, un Estado de Derecho fuerte, una sociedad civil dinámica y la evaluación de las amenazas y de las alertas tempranas constituyen los primeros pasos para contrarrestar la manipulación de la información y la injerencia; que, a pesar de todos los avances

realizados en la sensibilización respecto a la injerencia extranjera, muchas personas, incluidos los responsables políticos y los funcionarios que trabajan en los ámbitos que pueden ser objeto de ataques, siguen sin ser conscientes de los riesgos vinculados a la injerencia extranjera y del modo de abordarlos;

Q. Considerando que unos medios de comunicación independientes y de alta calidad financiados de manera sostenible y transparente, así como el periodismo profesional, son esenciales para la libertad y el pluralismo de dichos medios y para el Estado de Derecho y, por tanto, constituyen un pilar de la democracia y el mejor antídoto contra la desinformación; que algunos agentes extranjeros se aprovechan de la libertad de los medios de comunicación occidentales para difundir campañas de desinformación; que los medios de comunicación profesionales y el periodismo tradicional, como fuente de información de calidad, se enfrentan a tiempos difíciles en la era digital; que son necesarias una educación y una formación periodísticas de calidad dentro y fuera de la Unión con el fin de producir unos análisis periodísticos valiosos y unos estándares editoriales exigentes; que la Unión debe seguir apoyando el periodismo responsable en el entorno digital; que la comunicación basada en datos debe desempeñar un papel fundamental;

R. Considerando que los medios de comunicación de servicio público independientes desde el punto de vista editorial son fundamentales e insustituibles a la hora de prestar un servicio de información de alta calidad e imparcial al público en general y que deben ser protegidos de la captación maligna y reforzados como pilar fundamental de la lucha contra la desinformación;

S. Considerando que las distintas partes interesadas e instituciones utilizan metodologías y definiciones diferentes para analizar la injerencia extranjera, todas ellas con distintos grados de inteligibilidad, y que estas diferencias pueden inhibir la supervisión, el análisis y la evaluación comparables del nivel de amenaza, lo que dificulta la acción conjunta; que son necesarias una definición y una metodología de la Unión para mejorar el análisis común de las amenazas;

T. Considerando que es necesario complementar la terminología centrada en el contenido, como las noticias falsas o engañosas, la información errónea y la desinformación, con terminología centrada en la conducta, con el fin de abordar adecuadamente el problema; que esta terminología debe armonizarse y respetarse cuidadosamente;

U. Considerando que la formación en alfabetización mediática y digital y la sensibilización, tanto en el caso de los niños como en el de los adultos, son herramientas importantes para dotar a los ciudadanos de mayor resiliencia frente a los intentos de injerencia en el ámbito de la información y evitar la manipulación y la polarización; que, en general, las sociedades con un elevado nivel de alfabetización mediática son más resilientes a la injerencia extranjera; que los métodos de trabajo periodísticos, como el periodismo constructivo, podrían contribuir a reforzar la confianza en el periodismo entre los ciudadanos;

V. Considerando que la manipulación de la información puede adoptar muchas formas, como la propagación de desinformación y noticias totalmente falsas, la distorsión de hechos, narrativas y manifestaciones de opinión, la supresión de determinadas

informaciones u opiniones, la práctica de sacar la información de contexto, la manipulación de los sentimientos de las personas, la incitación al odio, la promoción de ciertas opiniones a expensas de otras y el acoso a las personas para silenciarlas; que uno de los objetivos de la manipulación de la información es crear caos para fomentar la pérdida de confianza de los ciudadanos en los «guardianes» de la información, tanto los nuevos como los antiguos; que hay una fina línea entre la libertad de expresión y la promoción del discurso de odio y la desinformación que no debe cruzarse;

W. Considerando que Azerbaiyán, China, Turquía y Rusia, entre otros países, han perseguido a periodistas y opositores en la Unión, como en el caso del bloguero y opositor azerbaiyano Mahammad Mirzali en Nantes o en el del periodista turco Erk Acarer en Berlín;

X. Considerando que existen pruebas concretas de que los procesos democráticos de la Unión son objeto de campañas de desinformación que ponen en tela de juicio los ideales democráticos y los derechos fundamentales; que la desinformación relacionada con temas como el género, las personas LGBTIQ +, la salud y los derechos sexuales y reproductivos y las minorías constituye una forma de desinformación que amenaza los derechos humanos, socava los derechos digitales y políticos, así como la seguridad y la protección de sus objetivos, y siembra la división y la desunión entre los Estados miembros; que, durante las campañas electorales, las candidatas políticas tienden a ser, de manera desproporcionada, objetivo de discursos sexistas, lo que desanima a las mujeres a participar en los procesos democráticos; que los autores de estas campañas de desinformación, so pretexto de promover valores «tradicionales» o «conservadores», forjan alianzas estratégicas con socios locales para acceder a la información disponible a escala local y, según se ha informado, reciben millones de euros en financiación extranjera;

Y. Considerando que, junto a las instituciones estatales, los periodistas, los líderes de opinión y el sector privado, cada sector de la sociedad y cada individuo desempeñan papeles relevantes para detener la propagación de desinformación y advertir a las personas de su entorno que se encuentran en situación de riesgo; que la sociedad civil, el mundo académico y los periodistas ya han contribuido en gran medida a sensibilizar a la opinión pública y aumentar la resiliencia de la sociedad, también en cooperación con sus homólogos de los países socios;

Z. Considerando que las organizaciones de la sociedad civil que representan las voces de las minorías y las organizaciones de derechos humanos en toda Europa siguen sin recibir suficiente financiación, a pesar de desempeñar un papel crucial en la sensibilización y la lucha contra la desinformación; que las organizaciones de la sociedad civil deben contar con recursos adecuados para desempeñar su papel en la limitación del impacto de las injerencias extranjeras;

AA. Considerando que es importante facilitar el acceso oportuno a la información basada en hechos y procedente de fuentes fiables cuando la desinformación comienza a propagarse;

AB. Considerando que es necesario detectar rápidamente los ataques de injerencia extranjera y los intentos de manipular el ámbito de la información para contrarrestarlos; que el

análisis de la información y la conciencia situacional en la Unión dependen de la voluntad de los Estados miembros de compartir información; que la presidenta de la Comisión Europea ha propuesto que se valore la posibilidad de crear un centro común de conciencia situacional de la Unión; que la prevención, medidas proactivas como la intervención preventiva frente a la desinformación y un ecosistema informativo saludable resultan mucho más eficaces que los esfuerzos de verificación de datos y refutación *a posteriori*, que han demostrado tener un alcance mucho menor que la desinformación original; que la Unión y sus Estados miembros carecen actualmente de las capacidades suficientes para adoptar tales medidas; que nuevas herramientas analíticas basadas en la inteligencia artificial, como el sitio web lituano Debunk.eu, podrían ayudar a detectar ataques, compartir conocimientos e informar al público;

AC. Considerando que la desinformación se alimenta, en un entorno de narrativas débiles o fragmentadas a escala nacional o de la Unión, de debates polarizados y emocionales, aprovechando los puntos débiles y los sesgos de la sociedad y los ciudadanos, y que la desinformación distorsiona el debate público en torno a las elecciones y otros procesos democráticos y puede dificultar a los ciudadanos la adopción de decisiones informadas;

***Injerencias extranjeras mediante el uso de plataformas en línea***

AD. Considerando que las plataformas en línea pueden representar herramientas fácilmente accesibles y asequibles para quienes se dedican a la manipulación de la información y otras injerencias, como la incitación al odio y el acoso, el perjuicio de la salud y la vulneración de la seguridad de nuestras comunidades en línea, el silenciamiento de los oponentes, el espionaje o la propagación de la desinformación; que se ha demostrado que su funcionamiento fomenta las opiniones polarizadas y extremas en detrimento de la información basada en hechos; que estas plataformas tienen también intereses particulares y pueden no ser neutrales en el tratamiento de la información; que algunas plataformas en línea se benefician enormemente del sistema que amplifica la división, el extremismo y la polarización; que el espacio en línea se ha vuelto tan importante para nuestra democracia como el espacio físico y, por lo tanto, requiere sus correspondientes normas;

AE. Considerando que las plataformas han acelerado y exacerbado la propagación de información errónea y desinformación de un modo inédito y complejo; que las plataformas en línea controlan el flujo de información y publicidad en la red, que diseñan y utilizan algoritmos para controlar tales flujos y que no son transparentes, carecen de los procedimientos adecuados para verificar la identidad, usan una terminología poco clara y ambigua y comparten muy poca o ninguna información sobre el diseño, el uso y los efectos de estos algoritmos; que el componente adictivo de los algoritmos de las plataformas en línea ha creado un grave problema de salud pública que debe abordarse; que las plataformas en línea deben responsabilizarse de los efectos perjudiciales de sus servicios, ya que algunas plataformas eran conscientes de las deficiencias de sus algoritmos, en particular su papel en la difusión de contenidos controvertidos, pero no las abordaron con el fin de maximizar sus beneficios, como han puesto de manifiesto los denunciantes de irregularidades;

AF. Considerando que existen campañas de injerencia y manipulación de la información centradas en todas las medidas contra la propagación de la COVID-19, incluida la vacunación en toda la Unión, y que las plataformas en línea no han logrado coordinar

sus esfuerzos para reprimirlas e incluso puede que hayan contribuido a su difusión; que esta desinformación puede suponer una amenaza para la vida al disuadir a las personas de que se vacunen o al promover tratamientos falsos; que la pandemia ha exacerbado la lucha sistémica entre la democracia y el autoritarismo, impulsando a agentes estatales y no estatales autoritarios, como China y Rusia, a emplear una amplia gama de instrumentos evidentes y encubiertos en su intento de desestabilizar a sus homólogos democráticos; que los «Papeles de Facebook» han revelado el fracaso de la plataforma a la hora de hacer frente a la desinformación relacionada con las vacunas, incluso en lengua inglesa; que la situación es aún peor en el caso de la desinformación relacionada con las vacunas que no está en inglés; que este problema atañe a todas las plataformas;

AG. Considerando que numerosos proveedores registrados en la Unión venden «me gusta», seguidores, comentarios y referencias a elementos compartidos falsos a cualquier agente que desee impulsar artificialmente su visibilidad en línea; que resulta imposible identificar los usos legítimos de tales servicios, mientras que entre sus usos perjudiciales figuran la manipulación de elecciones y otros procesos democráticos, la promoción de estafas, la publicación de reseñas negativas de productos de la competencia, la defraudación a los anunciantes y la creación de un público falso que se utiliza para manipular las conversaciones, lanzar ataques personales e inflar artificialmente ciertos puntos de vista que de otro modo no recibirían atención; que hay regímenes extranjeros, como Rusia y China, que utilizan estas herramientas en línea a gran escala para influir en el debate público en los países europeos; que la desinformación puede desestabilizar la democracia europea;

AH. Considerando que las plataformas sociales, los dispositivos y las aplicaciones digitales recaban y almacenan enormes cantidades de datos personales muy detallados y, a menudo, sensibles, sobre cada usuario; que esta información puede utilizarse para predecir tendencias de comportamiento, reforzar sesgos cognitivos y orientar la toma de decisiones; que esta información se explota con fines comerciales; que las fugas de datos se producen repetidamente, en detrimento de la seguridad de las víctimas de dichas fugas, y que los datos pueden venderse en el mercado negro; que tales bases de datos podrían constituir minas de oro para los agentes malintencionados que deseen actuar contra grupos o individuos;

AI. Considerando que, en general, las plataformas están diseñadas para garantizar que optar por no compartir datos resulte poco intuitivo y engorroso y requiera mucho tiempo en comparación con la opción de compartirlos;

AJ. Considerando que las plataformas en línea están integradas en la mayoría de los ámbitos de nuestras vidas y que la difusión de información puede ejercer un enorme impacto en nuestro pensamiento y comportamiento, por ejemplo, en lo que atañe a las preferencias de voto, a las decisiones sociales y económicas y a la elección de fuentes de información y que estas elecciones decisivas de importancia pública están hoy condicionadas, de hecho, por los intereses comerciales de empresas privadas;

AK. Considerando que los mecanismos de optimización de algoritmos y otras funciones de las plataformas de medios sociales están diseñados para maximizar la implicación de los usuarios; que reiteradamente se denuncia que estas funciones promueven contenidos discriminatorios, que polarizan y radicalizan y mantienen a los usuarios en círculos

afines; que esto lleva a la radicalización gradual de los usuarios de las plataformas, así como al condicionamiento y a la contaminación de los procesos de debate colectivo, más que a la protección de los procesos democráticos y de las personas; que la actuación descoordinada de las plataformas ha dado lugar a discrepancias en sus acciones y ha permitido que la desinformación se propague entre las plataformas; que el modelo de negocio consistente en hacer dinero a través de la difusión de información polarizada y del diseño de algoritmos hacen que las plataformas sean un objetivo fácil para la manipulación por parte de agentes hostiles extranjeros; que las plataformas de redes sociales podrían diseñarse de forma diferente para fomentar una esfera pública en línea más saludable;

AL. Considerando que la creación de materiales de audio y vídeo ultrafalsificados es cada vez más fácil con la llegada de tecnologías asequibles y fáciles de usar y que la difusión de estos materiales puede convertirse en un problema cada vez mayor; que, sin embargo, en la actualidad el 90 % de la investigación se destina al desarrollo de ultrafalsificaciones y solo el 10 % a su detección;

AM. Considerando que los sistemas de autorregulación como el Código de Buenas Prácticas de la Unión en materia de Desinformación de 2018 han dado lugar a mejoras; que, no obstante, la confianza en la buena voluntad de las plataformas no funciona ni es eficaz y ha generado pocos datos significativos sobre su impacto global; que, además, las plataformas han adoptado medidas individuales que varían en grado y efecto, lo que ha dado lugar a puertas traseras a través de las cuales los contenidos pueden seguir difundiéndose en otros lugares a pesar de haber sido retirados; que es necesario un conjunto claro de normas y sanciones para que el Código de Buenas Prácticas tenga suficiente efecto en el entorno en línea;

AN. Considerando que el Plan de Acción para la Democracia Europea pretende reforzar el Código de Buenas Prácticas de 2018 y que, junto con la Ley de Servicios Digitales, se aleja del enfoque de autorregulación y pretende introducir más garantías y protecciones para los usuarios, aumentando la autonomía y superando la pasividad respecto a los servicios ofrecidos, introduciendo medidas para exigir mayor transparencia y rendición de cuentas a las empresas e imponiendo más obligaciones a las plataformas;

AO. Considerando que las medidas actuales contra las campañas de desinformación en las plataformas en línea no son eficaces ni disuasorias y que permiten que las plataformas continúen fomentando los contenidos discriminatorios y malintencionados;

AP. Considerando que las plataformas dedican recursos significativamente menores a la gestión de los contenidos en las lenguas menos habladas, e incluso a los que se ofrecen en lenguas de uso generalizado diferentes del inglés, en comparación con los recursos que dedican a los contenidos en inglés;

AQ. Considerando que los procedimientos de reclamación y apelación de las plataformas son generalmente inadecuados;

AR. Considerando que, en los últimos meses, varios agentes principales han acatado normas de censura, como en el caso de las elecciones parlamentarias rusas de septiembre de 2021, cuando Google y Apple retiraron las aplicaciones de votación inteligente de sus mercados en Rusia;

AS. Considerando que la falta de transparencia con respecto a las elecciones de algoritmos por parte de las plataformas hace imposible validar las afirmaciones de estas respecto a lo que hacen y al efecto de sus acciones para contrarrestar la manipulación de la información y las injerencias; que hay discrepancias entre el efecto declarado de sus esfuerzos en sus autoevaluaciones anuales y su eficacia real, como se pone de manifiesto en los recientes «Papeles de Facebook»;

AT. Considerando que la naturaleza no transparente de la publicidad dirigida lleva a que enormes volúmenes de publicidad en línea de marcas de renombre, a veces incluso de instituciones públicas, terminen en sitios web que promueven el terrorismo y albergan contenidos que incitan al odio y desinforman y a que esta publicidad financie el crecimiento dichos sitios sin el conocimiento o el consentimiento de los anunciantes;

AU. Considerando que el mercado de la publicidad en línea está controlado por un pequeño número de grandes empresas de tecnología publicitaria que se reparten el mercado, entre las que destacan Google y Facebook; que esta elevada concentración del mercado en unas pocas empresas está asociada a un fuerte desequilibrio de poder; que el uso de técnicas de ciberanzuelo y el poder de estos pocos agentes para determinar qué contenidos se monetizan y cuáles no, a pesar de que los algoritmos que utilizan no pueden explicar la diferencia entre desinformación y contenidos informativos normales, constituyen una amenaza para la diversificación de los medios de comunicación; que el mercado de la publicidad dirigida no es transparente en absoluto; que las empresas de tecnología publicitaria obligan a las marcas a cargar con la culpa por su negligencia a la hora de supervisar dónde se colocan los anuncios;

***Infraestructuras críticas y sectores estratégicos***

AV. Considerando que la gestión de las amenazas a infraestructuras críticas, especialmente cuando forman parte de una estrategia híbrida sincronizada y malintencionada, requiere esfuerzos coordinados y conjuntos entre varios sectores, a diferentes niveles (a escala de la Unión, nacional, regional y local) y en distintos momentos;

AW. Considerando que la Comisión ha propuesto una nueva Directiva para reforzar la resiliencia de las entidades críticas que prestan servicios esenciales en la Unión, que contiene una propuesta de lista de nuevos tipos de infraestructuras críticas; que la lista de servicios figurará en el anexo a la Directiva;

AX. Considerando que la creciente globalización de la división del trabajo y de las cadenas de producción ha dado lugar a carencias en la fabricación y de las cualificaciones en sectores clave de toda la Unión; que esta situación ha dado lugar a una elevada dependencia de la Unión respecto a las importaciones de numerosos productos esenciales y activos primarios procedentes del extranjero que pueden presentar vulnerabilidades intrínsecas; que la resiliencia de la cadena de suministro debe figurar entre las prioridades de los responsables políticos de la Unión;

AY. Considerando que las inversiones extranjeras directas —inversiones de terceros países y empresas extranjeras— en sectores estratégicos de la Unión, pero también en regiones vecinas, como los Balcanes Occidentales, en particular la adquisición por parte de China de estructuras críticas, han sido motivo de una creciente preocupación en los últimos años, habida cuenta del incremento de la importancia del nexo entre el comercio y la

seguridad; que estas inversiones suponen un riesgo de que se creen dependencias económicas y se produzca una pérdida de conocimientos en sectores industriales y de producción clave;

AZ. Considerando que la autonomía estratégica abierta de la Unión requiere el control de las infraestructuras estratégicas europeas; que la Comisión y los Estados miembros han expresado una creciente preocupación por la seguridad y el control de las tecnologías y las infraestructuras en Europa;

***Injerencia extranjera durante los procesos electorales***

BA. Considerando que los agentes malintencionados que buscan interferir en los procesos electorales se aprovechan de la apertura y del pluralismo de nuestras sociedades como vulnerabilidad estratégica para atacar los procesos democráticos y la resiliencia de la Unión y sus Estados miembros; que es en el contexto de los procesos electorales donde la injerencia extranjera resulta más peligrosa a medida que los ciudadanos vuelven a involucrarse y se implican más en la participación política convencional;

BB. Considerando que el carácter distintivo de las injerencias extranjeras en los procesos electorales y el uso de las nuevas tecnologías en este sentido, así como sus posibles efectos, representan amenazas especialmente peligrosas para la democracia; que la injerencia extranjera en los procesos electorales va mucho más allá de la «guerra informativa» en las redes sociales, favoreciendo a determinados candidatos para piratear y atacar bases de datos y acceder a información de los votantes inscritos e interfiriendo directamente en el funcionamiento normal del proceso electoral, su competitividad y su legitimidad; que la injerencia extranjera tiene por objeto suscitar dudas, incertidumbre y desconfianza, y no solo alterar el resultado de las elecciones, sino también deslegitimar todo el proceso electoral;

***Financiación encubierta de actividades políticas por agentes y donantes extranjeros***

BC. Considerando que hay un cúmulo de pruebas sólidas que demuestran que ha habido una injerencia activa por parte de agentes extranjeros en el funcionamiento democrático de la Unión y sus Estados miembros, especialmente durante los períodos de elecciones y referendos, a través de operaciones de financiación encubiertas;

BD. Considerando, por ejemplo, que Rusia, China y otros regímenes autoritarios han destinado más de 300 millones USD a 33 países para interferir en los procesos democráticos, y que otros agentes, como Irán, Venezuela y agentes procedentes de Oriente Próximo y de la extrema derecha estadounidense, también han participado en la financiación encubierta; que esta tendencia se está acelerando claramente; que la mitad de estos casos atañen a acciones de Rusia en Europa; que la corrupción y el blanqueo de capitales ilícitos son una fuente de financiación política de terceros países autoritarios;

BE. Considerando que las herramientas mediáticas creadas por donantes extranjeros de forma poco transparente han resultado muy eficaces para obtener un gran número de seguidores y generar participación;

BF. Considerando que estas operaciones financian a partidos extremistas, populistas y antieuropeos y a otros partidos, personas o movimientos cuyo propósito es intensificar

la fragmentación social y socavar la legitimidad de las autoridades públicas europeas y nacionales; que esto ha contribuido a aumentar el alcance de estos partidos y movimientos;

BG. Considerando que Rusia pretende establecer contactos con partidos, personalidades y movimientos, con el fin de apoyarse en agentes de dentro de las instituciones de la Unión para legitimar las posiciones rusas y los Gobiernos interpuestos y presionar para que se atenúen las sanciones y se mitiguen las consecuencias del aislamiento internacional; que partidos como el austriaco Freiheitliche Partei Österreichs, el francés Rassemblement National y la Lega Nord italiana han firmado acuerdos de cooperación con el partido Rusia Unida del presidente Vladimir Putin y se enfrentan ahora a acusaciones de los medios de comunicación de que están dispuestos a aceptar financiación política de Rusia; que otros partidos europeos, como el alemán Alternative für Deutschland (AfD), los húngaros Fidesz y Jobbik y el Partido del Brexit en el Reino Unido, mantienen también un estrecho contacto con el Kremlin y que la AfD y Jobbik también han trabajado como «observadores electorales» en las elecciones controladas por Kremlin, por ejemplo en Donetsk y Luhansk, en el este de Ucrania, para supervisar y legitimar las elecciones patrocinadas por Rusia; que las conclusiones sobre los contactos estrechos y regulares entre funcionarios rusos y representantes de un grupo de secesionistas catalanes en España, así como entre funcionarios rusos y el mayor donante privado para la campaña salida del Reino Unido de la Unión Europea, requieren una investigación en profundidad y forman parte de la estrategia más amplia de Rusia para aprovechar todas y cada una de las oportunidades para manipular el discurso con el fin de promover la desestabilización;

BH. Considerando que el Grupo de Estados contra la Corrupción (GRECO) del Consejo de Europa y la Comisión de Venecia ya formularon amplias recomendaciones para reducir el margen de posible injerencia de agentes extranjeros a través de la financiación política;

BI. Considerando que las leyes electorales, y en particular las disposiciones sobre la financiación de las actividades políticas, no están suficientemente bien coordinadas a escala de la Unión y, por tanto, permiten métodos de financiación opacos por parte de agentes extranjeros; que la definición jurídica de las donaciones políticas es demasiado restringida, lo que permite que haya contribuciones extranjeras en especie en la Unión;

BJ. Considerando que, en algunos Estados miembros, la publicidad política en línea no está sujeta a las normas aplicables a la que se ofrece fuera de línea; que existe una grave falta de transparencia en la publicidad política en línea, lo que hace imposible que los reguladores vigilen el cumplimiento de los límites de gasto y eviten las fuentes ilegales de financiación, con consecuencias potencialmente desastrosas para la integridad de nuestros sistemas electorales;

BK. Considerando que la falta de transparencia en la financiación crea un entorno para la corrupción que suele acompañar a la financiación y las inversiones extranjeras;

BL. Considerando que el Reglamento (UE, Euratom) n.º 1141/2014, de 22 de octubre de 2014, sobre el estatuto y la financiación de los partidos políticos europeos y las

fundaciones políticas europeas[9] está siendo revisado con vistas a lograr un mayor nivel de transparencia en la financiación de las actividades políticas;

BM. Considerando que el papel de las fundaciones políticas ha crecido en los últimos años, que en la mayoría de los casos desempeñan un papel positivo en la política y en el fortalecimiento de la democracia, pero que en algunos casos se convierten en un vehículo más imprevisible de formas malintencionadas de financiación e injerencia indirecta;

BN. Considerando que las tecnologías modernas y los activos digitales, como las criptomonedas, se utilizan para encubrir transacciones financieras ilegales a actores políticos y a partidos políticos;

***Ciberseguridad y resiliencia frente a ciberataques***

BO. Considerando que la incidencia de ciberataques y ciberincidentes provocados por agentes estatales y no estatales hostiles ha aumentado en los últimos años; que se ha rastreado que el origen de varios ciberataques, como las campañas de correo electrónico de *phishing* personalizado a escala mundial dirigidas a estructuras estratégicas de almacenamiento de vacunas y los ataques informáticos contra la Agencia Europea de Medicamentos (EMA), la Autoridad Bancaria Europea, el Parlamento noruego y muchos otros, se encuentra en grupos de piratas informáticos que cuentan con respaldo estatal, afiliados en su mayoría a los Gobiernos ruso y chino;

BP. Considerando que la Unión Europea está comprometida con la aplicación en el ciberespacio de la legislación internacional vigente, en particular la Carta de las Naciones Unidas; que los agentes extranjeros malevolentes están aprovechando la ausencia de un marco jurídico internacional sólido en el ámbito cibernético;

BQ. Considerando que los Estados miembros han aumentado la cooperación en el ámbito de la ciberdefensa en el marco de la Cooperación Estructurada Permanente (CEP), en particular a través de la constitución de equipos de respuesta rápida a las ciberamenazas; que el Programa Europeo de Desarrollo Industrial en materia de Defensa (PEDID) ha incluido en sus programas de trabajo la inteligencia, la comunicación segura y la ciberdefensa; que la capacidad actual para hacer frente a las ciberamenazas es limitada debido a la escasez de recursos humanos y financieros, por ejemplo en estructuras críticas como los hospitales; que la Unión se ha comprometido a invertir 1 600 millones EUR, en el marco del programa Europa Digital[10], en la capacidad de respuesta y el despliegue de herramientas de ciberseguridad para las administraciones públicas, las empresas y las personas, así como a desarrollar la cooperación entre los sectores público y privado;

BR. Considerando que las lagunas y la fragmentación de las capacidades y estrategias de la Unión en el ámbito cibernético se están convirtiendo en un problema cada vez mayor, como señala el Tribunal de Cuentas Europeo[11]; que el conjunto de instrumentos de

[9] DO L 317 de 4.11.2014, p. 1.
[10] https://www.consilium.europa.eu/es/policies/cybersecurity/.
[11] https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_ES.pdf.

ciberdiplomacia de la Unión, creado en mayo de 2019, ha demostrado el valor añadido de una respuesta diplomática conjunta de la Unión a las actividades informáticas malintencionadas; que, el 30 de julio de 2020, el Consejo decidió por primera vez imponer medidas restrictivas contra personas, entidades y órganos responsables de diversos ciberataques o implicados en ellos;

BS. Considerando que agentes de Estados extranjeros han utilizado programas de vigilancia de uso ilícito a gran escala, como Pegasus, contra periodistas, activistas de derechos humanos, personalidades del mundo académico, funcionarios gubernamentales y políticos, incluidos jefes de Estado europeos; que los Estados miembros también han hecho uso de programas espía de vigilancia;

***Protección de los Estados miembros, instituciones, agencias, delegaciones y misiones de la Unión***

BT. Considerando que el carácter descentralizado y multinacional de las instituciones de la Unión, incluidos sus misiones y operaciones, se está convirtiendo cada vez más en un objetivo y es aprovechado por agentes extranjeros malintencionados que desean sembrar la división en la Unión; que hay una carencia general de cultura en materia de seguridad en las instituciones de la Unión, a pesar de que son objetivos claros; que el Parlamento, como institución de la Unión elegida democráticamente, se enfrenta a retos específicos; que varios casos han revelado que las instituciones de la Unión parecen vulnerables a la infiltración extranjera; que debe garantizarse la seguridad del personal de la Unión;

BU. Considerando que es necesario aplicar, con carácter prioritario, procedimientos rigurosos y coherentes de gestión de crisis; que debe ofrecerse formación adicional para mejorar la preparación del personal;

BV. Considerando que los ciberataques se han dirigido recientemente a varias instituciones de la Unión, lo que pone de relieve la necesidad de una estrecha cooperación interinstitucional en lo que atañe a la detección, al seguimiento y al intercambio de información durante los ciberataques y con vistas a prevenirlos, también durante las misiones y operaciones de la política común de seguridad y defensa (PCSD) de la Unión; que la Unión y los Estados miembros deben organizar ejercicios conjuntos y periódicos para detectar puntos débiles y adoptar las medidas necesarias;

***Injerencia por medio de agentes globales a través de la captación de élites, las diásporas nacionales, universidades y actos culturales***

BW. Considerando que varios políticos, incluidos antiguos políticos y funcionarios europeos de alto nivel, han sido contratados o captados por empresas públicas o privadas extranjeras controladas por Estados autoritarios, a cambio de sus conocimientos y en detrimento de los intereses de los ciudadanos de la Unión y de sus Estados miembros;

BX. Considerando que algunos países son especialmente activos en el ámbito de la captación y el reclutamiento de élites, en particular, Rusia y China, pero también Arabia Saudí y otros países del Golfo, y que, por ejemplo, el excanciller alemán Gerhard Schröder y el ex primer ministro de Finlandia Paavo Lipponen se incorporaron a Gazprom para agilizar el proceso de solicitud de Nord Stream 1 y 2, que la ex ministra austriaca de Asuntos Exteriores Karin Kneissl fue nombrada miembro del consejo de Rosneft, que el

ex primer ministro de Francia François Fillon fue nombrado miembro del consejo de Zaroubejneft, que el ex primer ministro de Francia Jean-Pierre Raffarin ha participado activamente en la promoción de los intereses chinos en Francia, que el excomisario checo Štefan Füle ha trabajado para CEFC China Energy, que el ex primer ministro de Finlandia Esko Aho ahora se sienta en el consejo del Sberbank —controlado por el Kremlin—, que el exministro francés de Relaciones con el Parlamento Jean-Marie Le Guen es actualmente miembro del Consejo de Administración de Huawei France, que el ex primer ministro de Bélgica Yves Leterme fue designado copresidente del fondo de inversión chino ToJoy, y que otros muchos políticos y funcionarios de alto nivel ocupan actualmente puestos parecidos;

BY. Considerando que las estrategias de representación de intereses en el ámbito económico pueden combinarse con objetivos de injerencia extranjera; que, según el informe de la Organización de Cooperación y Desarrollo Económicos (OCDE) sobre la representación de intereses en el siglo XXI[12], solo los Estados Unidos, Australia y Canadá cuentan con normas que abordan la injerencia extranjera; que hay una grave carencia de normas jurídicamente vinculantes y de aplicación del registro de representantes de intereses de la Unión, lo que hace imposible que se pueda rastrear la representación de intereses procedente de fuera de la Unión; que en la actualidad no hay forma de efectuar un seguimiento de las actividades de representación de intereses en los Estados miembros que influyen en la legislación y en la política exterior a través del Consejo Europeo; que las normas sobre la representación de intereses en la Unión se centran principalmente en el contacto presencial y no tienen en cuenta todo el ecosistema de los diferentes tipos de representación de intereses que existe en Bruselas; que, asimismo, países como China y Rusia, pero también Qatar, los Emiratos Árabes Unidos y Turquía, han realizado enormes inversiones en la representación de intereses en Bruselas;

BZ. Considerando que intentar instrumentalizar a grupos vulnerables, en particular las minorías y diásporas nacionales que residen en el territorio de la Unión, constituye un elemento importante de las estrategias de injerencia extranjera;

CA. Considerando que diversos agentes estatales, como los Gobiernos ruso y chino y, en menor medida, turco, han tratado de potenciar su influencia creando y utilizando instituciones culturales, educativas (p. ej., mediante subvenciones y becas) y religiosas en los Estados miembros, en un intento estratégico por desestabilizar la democracia europea y expandir su control sobre Europa central y oriental; que la supuesta difícil situación de su minoría nacional ha sido utilizada en el pasado por Rusia como excusa para la intervención directa en terceros países;

CB. Considerando que existen pruebas de las injerencias y la manipulación de la información en línea rusas en muchas democracias liberales de todo el mundo, incluidos, entre otros, los casos del referéndum del *Brexit* en el Reino Unido y las elecciones presidenciales en Francia y los Estados Unidos, así como el apoyo práctico a partidos extremistas, populistas y antieuropeos y a otros partidos y personas en toda

[12] Organización de Cooperación y Desarrollo Económicos: *Lobbying in the 21st Century: Transparency, Integrity and Access* (Representación de intereses en el siglo XXI: transparencia, integridad y acceso), 2021, OECD Publishing, París, disponible en: https://doi.org/10.1787/c6d8eff8-en.

Europa y, en particular, en Francia, Alemania, Italia y Austria; que es necesario más apoyo a la investigación y la educación para poder entender la influencia exacta de las injerencias extranjeras en acontecimientos específicos, como el *Brexit* y la elección del presidente Trump en 2016;

CC. Considerando que las redes Sputnik y RT controladas por el Estado ruso, con sede en Occidente, junto con medios de comunicación occidentales y total o parcialmente propiedad de personas físicas o jurídicas rusas y chinas, participan activamente en actividades de desinformación contra las democracias liberales; que Rusia recurre al revisionismo histórico, tratando de reescribir la historia de los crímenes soviéticos y de promover la nostalgia soviética entre la población sensible a la propaganda de Europa central y oriental; que, para las emisoras nacionales de Europa central y oriental, es difícil competir con contenido de televisión en lengua rusa financiado por el Gobierno ruso; que existe un riesgo de desequilibrio en la cooperación entre los medios de comunicación chinos y extranjeros, teniendo asimismo en cuenta que los medios chinos son la voz del Partido Comunista de China en el interior del país y fuera de él;

CD. Considerando que se han abierto más de quinientos centros Confucio en todo el mundo, incluidos unos doscientos en Europa, y que China utiliza los institutos Confucio y las aulas Confucio como herramienta de injerencia en la Unión; que en los institutos Confucio la libertad académica está gravemente limitada; que las universidades y programas educativos son objeto de una financiación extranjera masiva, en particular de China o Qatar, como es el caso del campus de la Universidad de Fudan en Budapest;

CE. Considerando que la Unión carece en la actualidad de las herramientas necesarias para hacer frente a la captación de élites y luchar contra el establecimiento de canales de influencia, también dentro de las instituciones de la Unión; que las capacidades de conciencia situacional y los instrumentos de contrainteligencia siguen siendo escasos a escala de la Unión y que se depende en gran medida de la voluntad de los agentes nacionales para compartir información;

***Disuasión, atribución y contramedidas colectivas, incluidas sanciones***

CF. Considerando que la Unión y sus Estados miembros no cuentan actualmente con un régimen específico de sanciones en relación con las injerencias extranjeras y las campañas de desinformación organizadas por agentes estatales extranjeros, lo que significa que estos agentes pueden suponer con seguridad que sus campañas de desestabilización contra la Unión no tendrán consecuencias;

CG. Considerando que garantizar una atribución clara de los ataques de desinformación y propaganda, incluida la publicación de los nombres de los autores, de sus patrocinadores y de los objetivos que pretenden lograr, y medir los efectos de estos ataques en el público destinatario constituyen los primeros pasos para defenderse eficazmente frente a estas acciones;

CH. Considerando que la Unión debe reforzar sus herramientas de disuasión, así como las de atribución y categorización de la naturaleza de estos ataques como contrarios o no al Derecho internacional, con el objetivo de establecer un régimen de sanciones eficaz para que los agentes extranjeros malintencionados tengan que pagar los costes de sus decisiones y asumir las consecuencias; que dirigirse a particulares podría no ser

suficiente; que, para proteger los procesos democráticos europeos frente a los ataques híbridos patrocinados por Estados, se podrían utilizar otras herramientas, como las medidas comerciales; que las medidas de disuasión deben aplicarse de manera transparente y con todas las garantías debidas; que los ataques híbridos se calibran de manera que caigan deliberadamente por debajo del umbral del artículo 42, apartado 7, del Tratado de la Unión Europea y del artículo 5 del Tratado del Atlántico Norte;

***Cooperación mundial y multilateralismo***

CI. Considerando que las acciones malintencionadas orquestadas por agentes estatales y no estatales extranjeros afectan a un gran número de países socios democráticos en todo el mundo; que los aliados democráticos dependen de su capacidad para aunar fuerzas en una respuesta colectiva;

CJ. Considerando que los países candidatos a la adhesión a la Unión de los Balcanes Occidentales se ven especialmente afectados por los ataques en forma de injerencias extranjeras y campañas de desinformación procedentes de Rusia, China y Turquía, como las campañas de injerencia de Rusia durante el proceso de ratificación del Acuerdo de Prespa en Macedonia del Norte; que China y Rusia han explotado la pandemia de COVID-19 en los Balcanes Occidentales para desestabilizar a estos países y desacreditar a la Unión; que se espera que los países candidatos y candidatos potenciales se adhieran a las iniciativas de la Unión para luchar contra las injerencias extranjeras;

CK. Considerando que socios y aliados de ideas afines siguen careciendo de una interpretación y unas definiciones comunes en lo que respecta a la naturaleza de las amenazas en cuestión; que el secretario general de las Naciones Unidas pide un código de conducta mundial para promover la integridad de la información pública; que la Conferencia sobre el Futuro de Europa constituye una plataforma importante para debatir sobre este asunto;

CL. Considerando que se requieren una cooperación y un apoyo multilaterales a escala mundial entre socios de ideas afines para hacer frente a las injerencias malintencionadas extranjeras; que otras democracias, como Australia y Taiwán, han desarrollado capacidades y estrategias avanzadas; que Taiwán ocupa un lugar destacado en la lucha contra la manipulación de la información, principalmente procedente de China; que el éxito del sistema taiwanés reside en la cooperación entre todas las ramas del Gobierno, pero también con ONG independientes especializadas en la verificación de datos y la alfabetización mediática y con plataformas de redes sociales, como Facebook, y en el fomento de la alfabetización mediática para todas las generaciones, la refutación de la desinformación y la limitación de la difusión de mensajes manipuladores; que la Comisión Especial INGE realizó una misión oficial de tres días a Taiwán para hablar sobre la desinformación y la intervención electoral extranjera;

***Necesidad de una estrategia coordinada de la Unión contra las injerencias extranjeras***

1. Expresa su profunda preocupación por la creciente incidencia y la naturaleza cada vez más sofisticada de las injerencias extranjeras y los intentos de manipulación de la información dirigidos contra todos los ámbitos del funcionamiento democrático de la Unión Europea y sus Estados miembros, llevados a cabo mayoritariamente por Rusia y

China;

2. Pide a la Comisión que proponga, y a los colegisladores y los Estados miembros que apoyen, una estrategia intersectorial coordinada y a múltiples escalas, así como la provisión de los recursos financieros adecuados, con el fin de dotar a la Unión y a sus Estados miembros de políticas adecuadas en materia de prospectiva y resiliencia y de herramientas de disuasión que les permitan hacer frente a todas las amenazas y ataques híbridos orquestados por agentes estatales y no estatales extranjeros; considera que esta estrategia debe basarse en:

   a) terminologías y definiciones comunes, una metodología única, evaluaciones y evaluaciones de impacto *ex post* de la legislación adoptada hasta la fecha, un sistema de inteligencia compartido, y comprensión, seguimiento, incluidas alertas tempranas, y conciencia situacional de las cuestiones en juego,

   b) políticas concretas que permitan el desarrollo de la resiliencia entre los ciudadanos de la Unión en consonancia con los valores democráticos, en particular mediante el apoyo a la sociedad civil,

   c) capacidades adecuadas de perturbación y defensa,

   d) respuestas diplomáticas y de disuasión, incluido un conjunto de instrumentos de la Unión para contrarrestar las operaciones de injerencia e influencia extranjeras, incluidas las operaciones híbridas, mediante medidas adecuadas como, por ejemplo, la atribución y la publicación del nombre de los autores, sanciones y contramedidas, y asociaciones mundiales para intercambiar prácticas y promover normas internacionales de comportamiento responsable de los Estados;

3. Subraya que todas las medidas para prevenir, detectar, atribuir y contrarrestar las injerencias extranjeras deben formularse de manera que se respeten y promuevan los derechos fundamentales, incluida la capacidad de los ciudadanos de la Unión para comunicarse de modo seguro, anónimo y sin censura, sin injerencias indebidas por parte de cualesquiera agentes extranjeros;

4. Considera que esta estrategia debe fundamentarse en un enfoque basado en el riesgo, en el conjunto de la sociedad y para toda la Administración, que abarque en particular los siguientes ámbitos:

   a) el refuerzo de la resiliencia mediante la conciencia situacional, la alfabetización mediática e informativa, el pluralismo de los medios de comunicación, el periodismo independiente y la educación,

   b) las injerencias extranjeras mediante el uso de plataformas en línea,

   c) las infraestructuras críticas y los sectores estratégicos,

   d) la injerencia extranjera durante los procesos electorales,

   e) la financiación encubierta de actividades políticas por agentes y donantes extranjeros,

f) la ciberseguridad y la resiliencia frente a los ciberataques,

g) la protección de los Estados miembros, instituciones, organismos, delegaciones y misiones de la Unión,

h) la injerencia por medio de agentes mundiales a través de la captación de élites, las diásporas nacionales, las universidades y los actos culturales,

i) la disuasión, la atribución y contramedidas colectivas, incluidas las sanciones,

j) la cooperación mundial y el multilateralismo;

5. Pide, en particular, a la Unión y a sus Estados miembros que impulsen los recursos y los medios asignados a los organismos y organizaciones de toda Europa y a escala mundial, como los grupos de reflexión y los verificadores de datos, encargados de hacer un seguimiento y sensibilizar sobre la gravedad de las amenazas, incluida la desinformación; destaca el papel crucial de la Unión en un sentido estratégico más amplio; pide que se refuerce la capacidad de prospectiva y la interoperabilidad de la Unión y sus Estados miembros para garantizar una preparación sólida con vistas a predecir, prevenir y mitigar la manipulación y las injerencias en la información extranjeras, reforzar la protección de sus intereses e infraestructuras estratégicos y participar en la cooperación y coordinación multilaterales para llegar a una comprensión común de la cuestión en los foros internacionales pertinentes; pide al Consejo de Asuntos Exteriores que debata periódicamente los asuntos de injerencia extranjera;

6. Expresa su preocupación por la abrumadora falta de concienciación también entre el público en general y los cargos públicos, de la gravedad de las amenazas actuales que plantean los regímenes autoritarios extranjeros y otros agentes malintencionados y que atañen a todas las escalas y sectores de la sociedad europea, concebidas para socavar los derechos fundamentales y la legitimidad de las autoridades públicas, ahondar la fragmentación política y social y, en algunos casos, incluso poner en peligro la vida de los ciudadanos de la Unión;

7. Se muestra preocupado por la ausencia de normas y de medidas apropiadas y suficientes para atribuir los actos de injerencia extranjera y responder a ellos, lo que da lugar a que los agentes malintencionados obtengan un cálculo atractivo de coste bajo, riesgo bajo y alta recompensa, ya que el riesgo de enfrentarse a represalias por sus acciones es actualmente muy escaso;

8. Insta a la Comisión a que incluya, cuando proceda, la perspectiva de las injerencias y la manipulación de la información extranjeras en la evaluación de impacto *ex ante* que se lleva a cabo antes de presentar nuevas propuestas, con miras a integrar la lucha contra las injerencias y la manipulación de la información extranjeras en la elaboración de las políticas de la Unión; insta a que el SEAE y la Comisión realicen asimismo revisiones periódicas sobre resiliencia y evalúen la evolución de las amenazas y su repercusión en la legislación y las políticas vigentes;

9. Pide a la Comisión que analice instituciones nacionales de reciente creación, como el Coordinador Nacional de Lucha contra las Injerencias Extranjeras de Australia, el Comité de Seguridad de Finlandia que asiste al Gobierno y a los ministerios, la Agencia

de Contingencias Civiles de Suecia, la nueva agencia para la defensa psicológica y el Centro Nacional de China, la nueva agencia nacional francesa Viginum, el Centro Nacional de Ciberseguridad de Lituania, y el Grupo de Trabajo de Coordinación en materia de Desinformación interagencias de Taiwán, para aprender de estas buenas prácticas y determinar en qué medida podría aplicarse una idea similar a escala de la Unión; anima a la Comisión a que respalde el intercambio de información y de mejores prácticas entre los Estados miembros en este sentido; subraya la importancia de unos enfoques e instrumentos proactivos, incluidas las comunicaciones estratégicas, como actividad esencial para aplicar las políticas de la Unión y de los Estados miembros mediante palabras y acciones; pide a la Comisión que proporcione una formación adecuada de ciencia de datos y establezca en su seno un órgano único de seguimiento en materia de manipulación de la información;

10. Expresa su preocupación por las numerosas brechas y lagunas existentes en la legislación y las políticas actuales a escala nacional y de la Unión formuladas para detectar, prevenir y contrarrestar las injerencias extranjeras;

11. Observa que la Unión está financiando diversos proyectos y programas a largo plazo que se centran en combatir la desinformación a nivel tecnológico, jurídico, psicológico e informativo; pide a la Comisión que evalúe el impacto de estos proyectos y programas y su pertinencia;

12. Pide a la Comisión que cree un grupo de trabajo de la Comisión, encabezado por Věra Jourová como vicepresidenta de la Comisión encargada de Valores y Transparencia, dedicado a examinar la legislación y las políticas vigentes con el fin de identificar las brechas que puedan ser aprovechadas por agentes malintencionados, e insta a la Comisión a que las subsane; subraya que esta estructura debe cooperar con otras instituciones de la Unión y los Estados miembros a escala nacional, regional y local, y facilitar el intercambio de buenas prácticas; pide a la Comisión y al SEAE que consideren la posibilidad de crear un centro europeo para las amenazas de injerencia y la integridad de la Información, dotado de recursos suficientes e independiente, que identifique, analice y documente las operaciones de manipulación de la información y las amenazas de injerencia contra la Unión en su conjunto, aumente la conciencia situacional, desarrolle un centro de conocimiento especializado que sea una plataforma para la coordinación con la sociedad civil, el sector empresarial y las instituciones nacionales y de la Unión, y aumente la sensibilización de la opinión pública, entre otras cosas mediante informes periódicos sobre las amenazas sistémicas; insiste en que la creación de ese nuevo centro europeo para las amenazas de injerencia y la integridad de la información, independiente y dotado de recursos adecuados, debe aclarar y mejorar el papel de la división StratCom del SEAE y sus grupos de trabajo, como organismo estratégico del servicio diplomático de la Unión, y evitar el solapamiento de actividades; subraya que el mandato de la división StratCom del SEAE debe centrarse en el desarrollo estratégico de políticas exteriores para combatir las amenazas conjuntas actuales y emergentes y mejorar la cooperación con los socios internacionales en este ámbito; señala que la división StratCom del SEAE podría perseguir este objetivo en estrecha cooperación con el nuevo centro europeo para las amenazas de injerencia y la integridad de la información y con el nuevo grupo de trabajo de la Comisión;

13. Pide a todas las instituciones de la Unión y a los Estados miembros que empoderen a la

sociedad civil para que desempeñe un papel activo en la lucha contra las injerencias extranjeras; pide a todos los niveles y sectores de la sociedad europea que establezcan sistemas para que las organizaciones y los ciudadanos sean más resilientes frente a las injerencias extranjeras, y puedan detectar los ataques a tiempo y contrarrestarlos con la mayor eficacia posible, en particular mediante la educación y la sensibilización, dentro del marco de los derechos fundamentales y de manera transparente y democrática; señala, en este contexto, las buenas prácticas y el enfoque que implica a toda la sociedad adoptados por Taiwán; pide a todos los responsables de la toma de decisiones que proporcionen a la sociedad civil herramientas y financiación adecuadas para estudiar, exponer y combatir la influencia extranjera;

***Refuerzo de la resiliencia de la Unión mediante la conciencia situacional, la alfabetización mediática y la educación***

14. Incide en que las instituciones y los Estados miembros de la Unión necesitan sistemas sólidos, firmes e interconectados para detectar, analizar, rastrear y catalogar los incidentes de agentes estatales y no estatales que tratan de interferir en los procesos democráticos, con el fin de desarrollar la conciencia situacional y una interpretación inequívoca del tipo de conducta que la Unión y sus Estados miembros han de disuadir y abordar; pide que se realicen periódicamente investigaciones sociológicas y encuestas para hacer un seguimiento de la resiliencia y la alfabetización mediática, así como para comprender el apoyo y la percepción públicos de las narrativas de desinformación más comunes;

15. Subraya que es igualmente importante que las conclusiones extraídas de estos análisis no se detengan en el seno de grupos de especialistas en injerencias extranjeras, sino que, en la medida de lo posible, se compartan abiertamente con el público en general, y en especial, con las personas que desempeñan funciones sensibles, de manera que todos sean conscientes de los patrones de amenaza y puedan evitar los riesgos;

16. Subraya además que es necesario formular una metodología común para el desarrollo de la conciencia situacional, las alertas tempranas y la evaluación de amenazas, la recopilación sistemática de pruebas y la detección oportuna de la manipulación del entorno de información, así como el desarrollo de normas de atribución técnica, por ejemplo sobre autenticidad del contenido, con el fin de garantizar una respuesta eficaz;

17. Hace hincapié en la necesidad de que la Unión, en cooperación con los Estados miembros y trabajando de manera multilateral en los foros internacionales pertinentes, desarrolle una definición conceptual de las amenazas de injerencia a que se enfrenta la Unión; subraya que tal definición debe reflejar las tácticas, técnicas, procedimientos e instrumentos utilizados para describir los patrones de comportamiento de los agentes estatales y no estatales de amenazas que observamos hoy en día; insta a la Comisión a que asocie a la Agencia de los Derechos Fundamentales de la Unión Europea a fin de garantizar que no se han integrado conceptos ni sesgos discriminatorios o no equitativos en las definiciones conceptuales;

18. Subraya que la diplomacia pública y la comunicación estratégica son elementos esenciales de las relaciones exteriores de la Unión y de la protección de sus valores democráticos; pide a las instituciones de la UE que sigan desarrollando e impulsando la

importante labor de la división StratCom del SEAE, con sus grupos de trabajo, del Centro de Inteligencia y de Situación de la Unión Europea (INTCEN) y la Célula de Fusión de la UE contra las Amenazas Híbridas, de la Dirección de Información del Estado Mayor de la Unión Europea y del sistema de alerta rápida, la cooperación establecida a escala administrativa entre el SEAE, la Comisión y el Parlamento, la red dirigida por la Comisión contra la desinformación, el grupo de trabajo administrativo del Parlamento contra la desinformación, y la cooperación en curso con la OTAN, el G7, la sociedad civil y las empresas privadas en lo que respecta a la coordinación en materia de inteligencia, el análisis, la puesta en común de buenas prácticas y la sensibilización sobre la manipulación de información y las injerencias extranjeras; acoge con satisfacción el Informe Especial 09/2021 del Tribunal de Cuentas Europeo (TCE) titulado «El impacto de la desinformación en la UE: una cuestión abordada, pero no atajada»; pide al SEAE y a la Comisión que publiquen un calendario detallado para la aplicación de las recomendaciones del TCE;

19. Subraya la necesidad de redoblar los esfuerzos de seguimiento permanente y de intensificarlos mucho antes de la celebración de elecciones, referéndums u otros procesos políticos importantes en toda Europa;

20. Pide a los Estados miembros que aprovechen plenamente estos recursos mediante la puesta en común de la información de inteligencia pertinente con el INTCEN y la participación activa en el sistema de alerta rápida; opina que el análisis y la cooperación en materia de inteligencia en la Unión y con la OTAN deben reforzarse aún más, al tiempo que se dota a dicha cooperación de mayor transparencia y rendición de cuentas democrática, en particular compartiendo la información con el Parlamento;

21. Acoge favorablemente la idea de la presidenta de la Comisión von der Leyen de establecer un centro común de conciencia situacional para mejorar la prospectiva estratégica y la autonomía estratégica abierta de la Unión, y espera una aclaración ulterior de su organización y su misión; subraya que tal centro requeriría una cooperación activa con los servicios pertinentes de la Comisión, el SEAE, el Consejo, el Parlamento y las autoridades nacionales; reitera, no obstante, la importancia de evitar la duplicación del trabajo y el solapamiento con las estructuras de la Unión existentes;

22. Recuerda la necesidad de dotar al SEAE de un mandato reforzado y claramente definido y de los recursos necesarios para que la División de Comunicación Estratégica, Grupos de Trabajo y Análisis de la Información haga un seguimiento de la manipulación de la información y las injerencias y las aborde más allá de las fuentes extranjeras que cubren actualmente los tres grupos de trabajo, y pueda ampliar su cobertura geográfica aplicando un enfoque basado en el riesgo; pide con urgencia que el SEAE despliegue las capacidades adecuadas para abordar la manipulación de la información y las injerencias procedentes de China, en particular mediante la creación de un equipo específico para Extremo Oriente; subraya asimismo la necesidad de potenciar significativamente los conocimientos técnicos especializados y la capacidad lingüística respecto a China y otras regiones de importancia estratégica, tanto en el SEAE, como en los Estados miembros y en las instituciones de la Unión en general, y de usar fuentes de información de inteligencia de código abierto, que en la actualidad están infrautilizadas;

23. Destaca la importancia de unos medios de comunicación de amplia difusión,

competitivos y plurales, de unos periodistas, verificadores de datos e investigadores independientes y de unos medios de comunicación de servicio público fuertes para un debate democrático vivo y libre; acoge favorablemente las iniciativas encaminadas a reunir, formar y apoyar de otro modo a las organizaciones de periodistas, verificadores de datos e investigadores independientes de toda Europa, como el Observatorio Europeo de los Medios de Comunicación Digitales y la Dotación Europea para la Democracia, en particular, en las regiones de mayor riesgo; lamenta profundamente que el Observatorio Europeo de los Medios de Comunicación Digitales no abarque a los Estados bálticos; acoge con satisfacción, asimismo, las iniciativas destinadas a establecer unos indicadores de fiabilidad del periodismo y la verificación de datos que sean fáciles de reconocer, como los iniciados por Reporteros sin Fronteras; pide a la Comisión que luche contra la propiedad monopolística de los medios de comunicación de masas;

24. Elogia la investigación indispensable y las numerosas iniciativas creativas y exitosas de alfabetización digital y mediática y de sensibilización llevadas a cabo por particulares, escuelas, universidades, organizaciones de medios de comunicación, instituciones públicas y organizaciones de la sociedad civil;

25. Pide a la Unión y a los Estados miembros que destinen fuentes de financiación pública de la Unión para los verificadores de datos, los investigadores, los periodistas y los medios de comunicación de calidad y de investigación independientes, y las ONG que estudian e investigan la manipulación de la información y las injerencias, promuevan la alfabetización mediática, digital y en información, y otros medios para empoderar a los ciudadanos, y estudian cómo medir de manera significativa la eficacia de la formación en materia de alfabetización mediática, digital y relativa a la información, la sensibilización, la refutación y la comunicación estratégica;

26. Pide medidas para fortalecer los medios de comunicación profesionales y plurales y garantizar que los editores reciban una remuneración justa por el uso de sus contenidos en internet; subraya que varios países de todo el mundo están tomando medidas para garantizar que los medios de comunicación dispongan de recursos financieros adecuados; reitera su llamamiento en favor de la creación de un fondo permanente de la Unión para los medios informativos y acoge con satisfacción, a este respecto, la iniciativa NEWS, incluidas las nuevas posibilidades de financiación para el sector de los medios de comunicación y la alfabetización mediática y en información en el programa Europa Creativa 2021-2027; observa, no obstante, que las fuentes de financiación pueden crear dependencia o afectar a la independencia de los medios de comunicación; destaca, a este respecto, la importancia de la transparencia de la financiación de los medios de comunicación; cree que, a fin de proteger el pluralismo de los medios de comunicación, es necesario revelar públicamente los datos relativos a quién posee o controla los medios de comunicación, les hace donaciones o les provee de contenidos, y quién paga los contenidos periodísticos;

27. Subraya la necesidad de elaborar y poner a disposición del público análisis, informes de incidentes y evaluaciones de amenazas públicas basadas en información de inteligencia sobre la manipulación de la información y las injerencias; propone, por lo tanto, la creación de una base de datos a escala de la Unión sobre incidentes de injerencias extranjeras notificados por las autoridades de la Unión y de los Estados miembros; subraya que la información sobre estos incidentes podría compartirse, cuando proceda,

con las organizaciones de la sociedad civil y el público en todas las lenguas de la Unión;

28. Pide a todos los Estados miembros que incluyan la alfabetización mediática y digital, así como la educación sobre la democracia, los derechos fundamentales, la historia reciente, los asuntos mundiales, el pensamiento crítico y la participación del público, en sus planes de estudio, desde los primeros años de instrucción hasta la educación de adultos, incluida la formación de profesores e investigadores; pide a la Comisión y a los Estados miembros que aumenten el apoyo a la educación y a la investigación históricas sobre la manera en que las injerencias extranjeras y el totalitarismo pasado han influido en la sociedad en general y, más concretamente, en los grandes acontecimientos democráticos;

29. Pide a las instituciones de la UE y a los Estados miembros, a todos los niveles administrativos, que identifiquen los sectores en riesgo de ser objeto de intentos de injerencia y ofrezcan periódicamente formación y prácticas al personal que trabaja en estos sectores sobre cómo detectar y evitar dichos intentos, y subraya que tales esfuerzos se beneficiarían de un formato normalizado establecido por la Unión; recomienda que se impartan módulos exhaustivos de formación a todos los funcionarios; acoge con satisfacción a este respecto la formación ofrecida a los diputados y al personal por la administración del Parlamento; recomienda que se siga desarrollando esta formación;

30. Subraya la necesidad de concienciar sobre las injerencias extranjeras en todas las capas de la sociedad; acoge con satisfacción las iniciativas emprendidas por el SEAE, la Comisión y la administración del Parlamento, como las actividades de formación y concienciación dirigidas a periodistas, profesores, influentes, estudiantes, ciudadanos mayores y visitantes, tanto en línea como fuera de línea, en Bruselas y en todos los Estados miembros, y recomienda que se sigan desarrollando;

31. Pide a los Estados miembros, a la administración de la Unión y a las organizaciones de la sociedad civil que compartan buenas prácticas en materia de formación para la alfabetización mediática y en información y la sensibilización, tal como se exige en la Directiva de servicios de comunicación audiovisual[13]; pide a la Comisión que organice estos intercambios en cooperación con el Grupo de Expertos en Alfabetización Mediática; subraya que los Estados miembros deben aplicar rápida y adecuadamente la Directiva revisada;

32. Insta a las instituciones de la Unión a que elaboren un código ético para orientar a las autoridades públicas y los representantes políticos en el uso de las plataformas y canales de redes sociales; considera necesario impulsar el uso responsable de esas plataformas y redes para luchar contra la manipulación y la información errónea que tienen su origen en el ámbito público;

33. Pide a la Unión y a sus Estados miembros que pongan en práctica programas a medida de concienciación y alfabetización mediática y en información, también para las

[13] Directiva 2010/13/UE del Parlamento Europeo y del Consejo, de 10 de marzo de 2010, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (DO L 95 de 15.4.2010, p. 1).

diásporas y las minorías, y pide asimismo a la Comisión que establezca un sistema para compartir fácilmente material en lenguas minoritarias, a fin de reducir los costes de traducción y llegar al mayor número posible de personas; pide a las regiones y municipios que asuman un papel de liderazgo, ya que es importante llegar a las zonas rurales y a todos los grupos demográficos;

34. Subraya que una respuesta esencial a los intentos de injerencia extranjera consiste en defender a los principales grupos a los que se dirige; hace hincapié en la necesidad de una acción específica, mediante un marco jurídico armonizado de la Unión, contra la propagación de la desinformación y el discurso del odio en cuestiones relacionadas con el género, las personas LGBTIQ+, las minorías y los refugiados; pide a la Comisión que elabore y aplique estrategias para dificultar la financiación de personas y grupos que participen activamente en la manipulación de la información o difundan activamente desinformación, frecuentemente dirigida contra los grupos y asuntos antes mencionados con el fin de dividir a la sociedad; pide campañas de comunicación positivas sobre estas cuestiones y subraya la necesidad de una formación que tenga en cuenta las cuestiones de género;

35. Reconoce que los ataques y las campañas de desinformación de género a menudo se utilizan como parte de una estrategia política más amplia para socavar la igualdad de participación en los procesos democráticos, en especial contra las mujeres y las personas LGBTIQ+; subraya que la desinformación sobre las personas LGBTIQ+ alimenta el odio, tanto en línea como fuera de línea. y pone en riesgo la vida de personas; pide que se lleve a cabo una investigación sobre la desinformación en línea con una perspectiva interseccional y que se supervisen los cambios que están realizando las plataformas para hacer frente a las campañas de desinformación de género en línea; pide que se preste una mayor atención a la desinformación de género mediante la creación de sistemas de alerta temprana a través de los cuales puedan denunciarse e identificarse campañas de desinformación de género;

36. Pide a la Comisión que proponga una estrategia global de alfabetización mediática y en información centrada especialmente en la lucha contra la manipulación de la información;

37. Celebra la creación de un grupo de expertos sobre la lucha contra la desinformación y el fomento de la alfabetización digital a través de la educación y la formación, que, entre otras tareas, se centre en el pensamiento crítico, la formación de los docentes, la intervención preventiva frente a la desinformación, la refutación y la verificación de datos, así como la participación de los estudiantes; pide a la Comisión que comparta los resultados del trabajo de este grupo de expertos y que ponga en práctica sus conclusiones;

38. Subraya la importancia de la comunicación estratégica para contrarrestar los discursos antidemocráticos más comunes; reclama una mejora de la comunicación estratégica de la Unión para aumentar su alcance, tanto respecto de sus ciudadanos como en el extranjero; incide en que todas las organizaciones democráticas han de defender la democracia y respetar el Estado de Derecho y deben asumir la responsabilidad común de interactuar con los ciudadanos, utilizando sus lenguas y plataformas preferidas;

39. Pide a los Estados miembros que garanticen campañas eficaces de comunicación pública en relación con la pandemia de COVID-19, con el fin de divulgar datos precisos y oportunos para combatir la información errónea, en particular la relativa a las vacunas;

40. Se muestra profundamente preocupado por la difusión de propaganda estatal extranjera, procedente principalmente de Moscú y Pekín, así como de Ankara, que se traduce a lenguas locales, por ejemplo, en contenidos mediáticos patrocinados por RT, Sputnik, Anadolu-, CCTV-, Global Times-, Xinhua-, TRT World, o el Partido Comunista Chino disfrazados de periodismo, y distribuidos en periódicos; sostiene que dichos canales no pueden ser considerados verdaderos medios de comunicación, por lo que no deberían disfrutar de los mismos derechos y protección que los medios de comunicación democráticos; preocupa asimismo el modo en que tales narrativas se han extendido a los productos periodísticos reales; subraya la necesidad de sensibilizar a la opinión pública acerca de las campañas de desinformación de Rusia y de China, cuyo objeto es desafiar los valores democráticos y dividir a la Unión, ya que constituyen la principal fuente de desinformación en Europa; pide a la Comisión que ponga en marcha un estudio sobre normas mínimas para los medios de comunicación, como base para la posible revocación de licencias en casos de incumplimiento; pide a la Comisión que integre las conclusiones de dicho estudio en la futura legislación, por ejemplo en una posible ley de libertad de los medios de comunicación; observa que los agentes de injerencias extranjeras pueden presentarse falsamente como periodistas; considera que, en tales casos, debe ser posible sancionar a esa persona u organización, por ejemplo, mediante la denuncia pública, la inclusión en listas negras para actos de prensa o la revocación de la acreditación de prensa;

41. Expresa su profunda preocupación por los ataques, el acoso, la violencia y las amenazas contra periodistas, defensores de los derechos humanos y otras personas que dan a conocer injerencias extranjeras, lo que también puede socavar su independencia; pide a la Comisión que presente rápidamente propuestas concretas y ambiciosas sobre la seguridad de todas estas personas, incluido un instrumento contra la demanda estratégica contra la participación pública y un apoyo económico, jurídico y diplomático, como se anunció en el Plan de Acción para la Democracia Europea; celebra, en este sentido, la Recomendación (UE) 2021/1534 de la Comisión, de 16 de septiembre de 2021, sobre la garantía de la protección, la seguridad y el empoderamiento de los periodistas y los otros profesionales de los medios de comunicación en la Unión Europea[14]; pide a los Estados miembros que protejan eficazmente a los periodistas y a otros profesionales de los medios comunicación mediante herramientas legislativas y no legislativas;

42. Subraya la necesidad de procurar la participación de los responsables de la toma de decisiones locales y regionales encargados de las decisiones estratégicas en los ámbitos de su competencia, como las infraestructuras, la ciberseguridad, la cultura y la educación; destaca que los políticos y las autoridades locales y regionales pueden identificar a menudo la evolución de los acontecimientos en una fase temprana, y subraya que, con frecuencia, se requieren conocimientos locales para identificar y

[14] DO L 331 de 20.9.2021, p. 8.

aplicar las contramedidas adecuadas;

43. Pide a la Comisión y a los Estados miembros que establezcan canales de comunicación y plataformas para que las empresas, las ONG y las personas, incluidos los miembros de las diásporas, puedan notificar situaciones en las que sean víctimas de la manipulación de la información o de injerencias; pide a los Estados miembros que apoyen a las víctimas de ataques, a las personas que tengan conocimiento de ellos y a las personas que se vean sometidas a presión;

***Injerencias extranjeras mediante el uso de plataformas en línea***

44. Acoge favorablemente la revisión propuesta del Código de Buenas Prácticas en materia de Desinformación y las propuestas de una Ley de servicios digitales, una Ley de mercados digitales y otras medidas vinculadas al Plan de Acción para la Democracia Europea como instrumentos potencialmente eficaces para luchar contra las injerencias extranjeras; recomienda que en la lectura final de estos textos se tengan en cuenta los aspectos expuestos en el resto de esta sección;

45. Subraya que la libertad de expresión no debe malinterpretarse como libertad para participar en actividades en línea que sean ilegales fuera de línea, como el acoso, el discurso del odio, la discriminación racial, el terrorismo y la violencia, el espionaje y las amenazas; incide en que las plataformas no solo han de atenerse a la ley del país en el que operan, sino también a sus términos y condiciones, en particular con respecto a los contenidos nocivos en línea; pide a las plataformas que redoblen sus esfuerzos para evitar la reaparición de contenidos ilegales idénticos a los que han sido identificados como ilegales y retirados;

46. Subraya la necesidad, sobre todo, de seguir estudiando el aumento de la desinformación y las injerencias extranjeras en línea y de que la legislación a escala de la Unión garantice un aumento significativo y significativo de la transparencia, el seguimiento y la rendición de cuentas en lo que respecta a las operaciones llevadas a cabo por las plataformas en línea y el acceso a los datos para los solicitantes de acceso legítimos, en particular a la hora de tratar los algoritmos y la publicidad en línea; pide a las empresas de redes sociales que mantengan bibliotecas de publicidad;

47. Pide que la regulación y las acciones obliguen a las plataformas, especialmente a las que presentan un riesgo sistémico para la sociedad, a hacer lo propio para reducir la manipulación y las injerencias en la información, por ejemplo mediante el uso de etiquetas que indiquen a los autores verdaderos detrás de las cuentas, limitando el alcance de las cuentas utilizadas habitualmente para difundir desinformación o que infrinjan regularmente los términos y las condiciones de la plataforma, suspendiendo y, en caso necesario y sobre la base de una legislación clara, suprimiendo cuentas inauténticas utilizadas para campañas de injerencia coordinadas o desmonetizando sitios de difusión de desinformación, estableciendo medidas de mitigación para los riesgos de injerencia que plantean los efectos de sus algoritmos, modelos de publicidad, sistemas de recomendación y tecnologías de IA, y señalando contenidos de desinformación tanto en las publicaciones como en los comentarios; recuerda la necesidad de que estas medidas se apliquen de una manera transparente y responsable;

48. Pide a la Comisión que tenga plenamente en cuenta la nota de orientación del Consejo

de Europa sobre mejores prácticas en favor de marcos jurídicos y procedimentales eficaces para mecanismos de autorregulación y corregulación de moderación de contenidos aprobada en junio de 2021;

49. Pide una aplicación más firme del Reglamento General de Protección de Datos[15], que limite la cantidad de datos que pueden almacenar las plataformas sobre los usuarios y el plazo en que estos datos pueden utilizarse, especialmente en las plataformas y aplicaciones que emplean datos muy privados y sensibles, como las de mensajería, salud, finanzas y citas y los pequeños grupos de debate; pide a las plataformas de guardianes de acceso que se abstengan de combinar datos personales con datos personales de otros servicios ofrecidos por el guardián de acceso o con datos personales de servicios de terceros, a fin de que sea igualmente fácil no estar de acuerdo con el almacenamiento y el intercambio de datos y permitir a los usuarios elegir si van dirigidos a otros tipos de publicidad personalizada en línea; acoge con satisfacción todos los esfuerzos realizados para prohibir las técnicas de microsegmentación para la publicidad política, en particular, pero no exclusivamente, las basadas en datos personales sensibles, como el origen étnico, las creencias religiosas o la orientación sexual, y pide a la Comisión que considere la posibilidad de ampliar la prohibición de la microsegmentación a la publicidad temática;

50. Pide normas vinculantes de la Unión que exijan a las plataformas que cooperen con las autoridades competentes para someter a pruebas sus sistemas regularmente y para identificar, evaluar y mitigar el riesgo de manipulación de la información e injerencias y las vulnerabilidades que conlleva el uso de sus servicios, además de cómo contribuye el diseño y la gestión de sus servicios a dicho riesgo; pide normas vinculantes de la Unión que obliguen asimismo a establecer sistemas para hacer un seguimiento de cómo se utilizan sus servicios, por ejemplo, un seguimiento en tiempo real de las entradas que generan más tendencia y son más populares en una panorámica país por país, con el fin de detectar los casos de manipulación de la información e injerencia y señalar las sospechas de injerencia a las autoridades competentes, y que aumenten los costes para los agentes que permiten que se pueda hacer la vista gorda ante tales acciones facilitadas por sus sistemas;

51. Pide a las plataformas en línea que asignen recursos adecuados para prevenir las injerencias extranjeras perjudiciales, así como para garantizar mejores condiciones de trabajo, atención psicológica y una remuneración justa para los moderadores de contenidos; pide a las grandes plataformas de redes sociales que faciliten informes detallados por país sobre los recursos dedicados a la verificación de datos a nivel nacional, las actividades de investigación, la moderación de contenidos, incluidas las capacidades humanas y de inteligencia artificial en cada lengua, y la colaboración con la sociedad civil local; subraya la necesidad de que estas plataformas redoblen sus esfuerzos para hacer frente a la desinformación en mercados más pequeños y menos comercialmente rentables de la Unión;

52. Pide a las plataformas de redes sociales que respeten plenamente la igualdad de todos

[15] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (DO L 119 de 4.5.2016, p. 1).

los ciudadanos de la Unión, independientemente de la lengua utilizada en el diseño de sus servicios, herramientas y mecanismos de seguimiento, así como en las medidas para una mayor transparencia y un entorno en línea más seguro; subraya que esto no solo se refiere a todas las lenguas oficiales nacionales y regionales, sino también a las lenguas de las diásporas importantes dentro de la Unión; subraya que estos servicios también deben ser accesibles para las personas con discapacidad auditiva;

53. pide un etiquetado claro y legible de las ultrafalsificaciones tanto para los usuarios de plataformas como en los metadatos de los contenidos con el fin de mejorar su trazabilidad para los investigadores y los verificadores de datos; acoge con satisfacción, a este respecto, las iniciativas destinadas a mejorar la autenticidad y trazabilidad de los contenidos, como el desarrollo de marcas de agua y normas de autenticidad, y la introducción de normas mundiales;

54. Pide que se regulen los servicios que ofrecen herramientas y servicios de manipulación de las redes sociales, como el aumento del alcance de las cuentas o los contenidos mediante la participación artificial o perfiles no auténticos; subraya que esta regulación debe basarse en una evaluación exhaustiva de las prácticas actuales y de los riesgos asociados y debe evitar que agentes malintencionados utilicen estos servicios para injerencias políticas;

55. Subraya la necesidad de transparencia respecto a las personas físicas o jurídicas reales que se encuentran detrás de los contenidos y las cuentas en línea cuando desean hacer publicidad; pide a las plataformas que introduzcan mecanismos para detectar y suspender, en particular, las cuentas no auténticas vinculadas a operaciones de ejercicio de influencia coordinadas; subraya que estas prácticas no deben interferir en la posibilidad del anonimato en línea, que resulta de fundamental importancia para proteger a periodistas, activistas, comunidades marginadas y personas en posiciones vulnerables (p. ej., denunciantes de irregularidades, disidentes y opositores políticos a regímenes autocráticos), y deben dar cabida a relatos satíricos y humorísticos;

56. Subraya que una mayor responsabilidad respecto a la eliminación de contenidos no debe dar lugar a la eliminación arbitraria de contenidos legales; insta a actuar con cautela respecto a la suspensión total de las cuentas de personas reales o al uso masivo de filtros automáticos; observa con preocupación las decisiones arbitrarias de las plataformas de eliminar las cuentas de cargos electos; recalca que estas cuentas solo deben eliminarse sobre la base de una normativa clara fundamentada en valores democráticos, traducidos en la política empresarial y cuyo respeto esté garantizado mediante un control democrático independiente, y que debe existir un proceso plenamente transparente que incluya el derecho de recurso;

57. Pide normas vinculantes que exijan a las plataformas que creen canales de comunicación fácilmente disponibles y eficaces para las personas u organizaciones que deseen denunciar contenidos ilegales, violación de los términos y condiciones, desinformación, manipulación de la información o injerencias extranjeras, cuando proceda, que permitan contestar a las personas acusadas antes de adoptar cualquier medida restrictiva, y que establezcan procedimientos de recurso, también de recurso judicial, imparciales, transparentes, rápidos y accesibles, tanto para las víctimas de contenidos publicados en línea como para las personas que informan sobre contenidos y

las personas u organizaciones afectadas por la decisión de etiquetar cuentas, restringir su visibilidad, desactivar el acceso a las mismas o suspenderlas, o limitar el acceso a los ingresos publicitarios; recomienda que las plataformas de redes sociales designen un punto de contacto específico para cada Estado miembro y creen equipos de trabajo para todas las elecciones importantes en cada uno de los Estados miembros;

58. Pide normas legislativas para garantizar la transparencia ante los usuarios y el público en general, como obligar a las plataformas a crear archivos públicos con funciones de búsqueda sencilla de anuncios en línea, que incluyan a quién están dirigidos y quién los ha pagado, y de contenidos moderados y eliminados, a establecer medidas de autorregulación y a proporcionar un acceso integral y significativo a la información sobre el diseño, el uso y el impacto de algoritmos a autoridades nacionales competentes, investigadores autorizados afiliados a instituciones académicas, medios de comunicación, organizaciones de la sociedad civil y organizaciones internacionales que representen intereses públicos; cree que los parámetros de estas bibliotecas deben armonizarse para permitir un análisis entre plataformas y reducir la carga administrativa para las plataformas;

59. Pide que se ponga fin a los modelos de negocio que se basan en animar a las personas a permanecer más tiempo en las plataformas alimentándolas con contenidos atractivos; pide a los responsables de la toma de decisiones y a las plataformas legislativas que garanticen, mediante el uso de moderadores humanos y de un auditor tercero, que los algoritmos no promuevan contenidos ilegales, extremistas, discriminatorios o radicalizadores, sino que ofrezcan a los usuarios una pluralidad de perspectivas y den prioridad y promuevan hechos y contenidos basados en la ciencia, en particular en cuestiones sociales importantes como la salud pública y el cambio climático; considera que los sistemas de clasificación adictivos y basados en la interacción suponen una amenaza sistémica para nuestra sociedad; pide a la Comisión que aborde el problema actual de los incentivos de precios, dado que anuncios muy dirigidos con contenidos divisivos a menudo tienen precios mucho más bajos para la misma cantidad de visionados que anuncios menos dirigidos con contenidos socialmente integradores;

60. Pide que se modifiquen los algoritmos para frenar la promoción de contenidos procedentes de cuentas y canales no auténticos que impulsan artificialmente la propagación de la manipulación nociva de la información por parte de agentes extranjeros; pide que se modifiquen los algoritmos para que no impulsen contenidos divisivos y que induzcan al enfado; subraya la necesidad de que la Unión ponga en marcha medidas para exigir legalmente a las empresas de redes sociales que eviten la amplificación de la desinformación una vez detectada en la mayor medida posible, y que debe haber consecuencias para las plataformas si no cumplen el requisito de eliminar la desinformación;

61. Subraya la necesidad de una mejora de la fase de pruebas y de una revisión sistemática de las consecuencias de los algoritmos, que incluya cómo configuran el discurso público e influyen en los resultados políticos y de qué manera se priorizan los contenidos; incide en que tal revisión debe examinar asimismo si las plataformas pueden cumplir las garantías prometidas en sus respectivos términos y condiciones, y si cuentan con suficientes salvaguardias para impedir que conductas no auténticas y coordinadas a gran escala manipulen el contenido mostrado en sus plataformas;

62. Se muestra alarmado ante el promedio de 65 millones EUR en ingresos por publicidad que fluyen cada año a aproximadamente 1 400 sitios web de desinformación dirigidos a ciudadanos de la Unión[16]; pone de relieve que anuncios en línea, en ocasiones incluso de instituciones públicas, acaban en sitios web malintencionados que promueven el discurso del odio y la desinformación, y que, por lo tanto, los financian, sin el consentimiento o incluso el conocimiento de los anunciantes en cuestión; observa que cinco empresas, incluida Google Ads, pagan el 97 % de estos ingresos por publicidad y se encargan de seleccionar los sitios web de los editores incluidos en su inventario y, por lo tanto, tienen el poder para determinar qué contenidos se monetizan y cuáles no; considera inaceptable que los algoritmos que distribuyen los fondos publicitarios sean una completa caja negra para el público; pide a la Comisión que haga uso de las herramientas de la política de competencia y de la legislación antimonopolio para garantizar un mercado funcional y romper este monopolio; pide a estos agentes que eviten que los sitios web que se dedican a la desinformación se financien con sus servicios publicitarios; felicita a las organizaciones dedicadas a promover la sensibilización respecto a esta cuestión preocupante; subraya que los anunciantes deben tener derecho a conocer y decidir dónde se colocan sus anuncios y qué intermediario ha tratado sus datos; pide el establecimiento de un proceso de mediación que permita a los anunciantes obtener un reembolso cuando los anuncios se coloquen en sitios web que promuevan la desinformación;

63. Subraya que el Código de Buenas Prácticas en materia de Desinformación actualizado, la Ley de servicios digitales, la Ley de mercados digitales y otras medidas vinculadas al Plan de Acción para la Democracia Europea requerirán una visión general y un mecanismo de evaluación y de sanciones eficaces tras su adopción, con el fin de evaluar su ejecución a escala nacional y de la Unión de manera periódica, de identificar y corregir las lagunas existentes sin demora y de sancionar la aplicación incorrecta y el incumplimiento de los compromisos; pide, a este respecto, unos coordinadores de servicios digitales sólidos y con recursos en cada Estado miembro, así como recursos suficientes para que el brazo de ejecución de la Comisión realice las tareas que le han sido asignadas por la Ley de servicios digitales; recalca, además, la importancia de velar por que las plataformas en línea se sometan a auditorías independientes certificadas por la Comisión; señala que los auditores no pueden ser financiados por plataformas individuales para garantizar su independencia;

64. Pide, a este respecto, que se definan indicadores clave de rendimiento por medio de corregulación, con el fin de garantizar la verificabilidad de las acciones adoptadas por las plataformas, así como sus efectos; subraya que estos indicadores clave de rendimiento deben incluir parámetros específicos por país, como el público al que se dirige la desinformación, la interacción (tasa de clics, etc.), la financiación de actividades de verificación de datos e investigación en el país, y la prevalencia y la fortaleza de las relaciones de la sociedad civil dentro del país;

65. Se muestra profundamente preocupado por la falta de transparencia en la revisión del Código de Buenas Prácticas en materia de Desinformación, ya que el debate se ha reservado en gran medida al sector privado y a la Comisión; lamenta que no se haya

[16] https://disinformationindex.org/wp-content/uploads/2020/03/GDI_Adtech_EU.pdf.

consultado adecuadamente al Parlamento Europeo, en particular a la Comisión Especial INGE, y a otras partes interesadas clave, durante la elaboración de la revisión del Código;

66. Lamenta el carácter autorregulador continuado del Código de Buenas Prácticas, ya que la autorregulación es insuficiente a la hora de proteger al público de las injerencias y los intentos de manipulación; manifiesta su preocupación por la posible incapacidad del Código de Buenas Prácticas en materia de Desinformación actualizado para proporcionar una respuesta a los retos futuros; se muestra preocupado por que las directrices para reforzar el Código de Buenas Prácticas dependan tanto de la propuesta de Ley de servicios digitales de la Comisión; pide que se emprendan acciones rápidas para garantizar que el Código de Buenas Prácticas incorpore compromisos vinculantes para las plataformas con el fin de garantizar la preparación de la Unión antes de las próximas elecciones locales, regionales, nacionales y europeas;

67. Pide que la Unión proteja y promueva el diálogo dentro de la comunidad tecnológica y el intercambio de información sobre el comportamiento y las estrategias de las plataformas sociales; considera que solo una comunidad tecnológica abierta puede reforzar la opinión pública contra ataques, manipulaciones e injerencias; pide que se estudie la posibilidad de crear un centro de puesta en común y análisis de la información público-privado para la desinformación, cuyos miembros rastreen, etiqueten y compartan información sobre amenazas relativas a contenidos de desinformación y sus agentes de difusión con arreglo a una clasificación de amenazas; cree que esto podría notificar al sistema de alerta rápida de la Unión y al mecanismo del G7 y también beneficiaría a agentes más pequeños con menos recursos; pide asimismo una norma a escala de la industria sobre desinformación para los servicios publicitarios y los servicios de monetización en línea con el fin de desmonetizar los contenidos nocivos, que también deberán utilizar los sistemas de pago en línea y las plataformas de comercio electrónico y que debe auditar un tercero;

68. Subraya la necesidad de que el Código pueda funcionar como herramienta eficaz hasta la entrada en vigor de la Ley de servicios digitales; cree que el Código debe anticipar algunas de las obligaciones de la Ley de servicios digitales y obligar a los firmantes a aplicar una serie de disposiciones de la Ley de servicios digitales en relación con el acceso a los datos para los investigadores y los reguladores y la transparencia de la publicidad, incluida la transparencia de los sistemas algorítmicos y de recomendación; insta a los firmantes a que auditen su cumplimiento de estas obligaciones con un auditor independiente y pide que se publiquen estos informes de auditoría;

69. Lamenta la falta de transparencia en el proceso para hacer un seguimiento del cumplimiento del Código, así como el calendario de la revisión del Código, que finalizará antes de la conclusión del mandato de la Comisión Especial INGE; observa que, como mínimo, deben publicarse los órdenes del día, las conclusiones y la lista de asistencia de las reuniones; insta a los firmantes a que declaren ante el Parlamento sus compromisos en relación con el Código y la manera en que han ejecutado y ejecutarán estos compromisos;

70. Considera que los reguladores independientes de los medios de comunicación, como el Grupo de Entidades Reguladoras Europeas para los Servicios de Comunicación

Audiovisual, podrían desempeñar un papel crucial en el seguimiento y la aplicación del Código;

71. Acoge favorablemente la propuesta de establecer un grupo de trabajo en las directrices de Comisión para reforzar el Código; insiste en que la Comisión invite a representantes del Parlamento, reguladores nacionales y otras partes interesadas, también de la sociedad civil y de la comunidad investigadora, a formar parte de este grupo de trabajo;

***Infraestructuras críticas y sectores estratégicos***

72. Considera que, dada su naturaleza interconectada y transfronteriza, las infraestructuras críticas son cada vez más vulnerables a interferencias externas, y cree que el marco vigente debe revisarse; acoge con satisfacción, en este sentido, la propuesta de la Comisión de una nueva directiva para reforzar la resistencia de las entidades críticas que prestan servicios esenciales en la Unión Europea;

73. Recomienda que los Estados miembros mantengan la prerrogativa de identificar las entidades críticas en su territorio, pero señala que es necesaria una coordinación a nivel de la Unión para:

a) consolidar los canales de conexión y comunicación utilizados por múltiples agentes, en particular para la seguridad general de las misiones y las operaciones de la Unión;

b) apoyar a las autoridades competentes de los Estados miembros a través del Grupo de Resiliencia de las Entidades Críticas, garantizando una participación diversa de las partes interesadas, en particular la implicación activa de las pymes, las organizaciones de la sociedad civil y los sindicatos;

c) promover el intercambio de mejores prácticas no solo entre los Estados miembros, sino también a nivel a escala regional y local, también con los Balcanes Occidentales, y entre propietarios y operadores de infraestructuras críticas, también a través de la comunicación entre agencias, con el fin de detectar en una fase temprana fenómenos preocupantes y desarrollar contramedidas adecuadas;

d) aplicar una estrategia común de respuesta a los ciberataques contra infraestructuras críticas;

74. Recomienda que la lista de entidades críticas se amplíe para incluir los medios de comunicación, las infraestructuras electorales digitales y los sistemas educativos, dada su importancia crucial en la tarea de garantizar el funcionamiento y la estabilidad a largo plazo de la Unión y sus Estados miembros, y que debería actuarse con flexibilidad al decidir sobre la incorporación a la lista de nuevos sectores estratégicos que deban protegerse;

75. Pide un enfoque global de la Unión para abordar los problemas de las amenazas híbridas a los procesos electorales y mejorar la coordinación y la cooperación entre los Estados miembros; pide a la Comisión que evalúe críticamente la dependencia respecto a las plataformas y la infraestructura de datos en el contexto de las elecciones; cree que falta control democrático sobre el sector privado; pide un mayor control democrático de las

plataformas, incluido el acceso adecuado de las autoridades competentes a datos y algoritmos;

76. Recomienda que las obligaciones derivadas de la directiva propuesta, incluidas las evaluaciones de amenazas, riesgos y vulnerabilidades a escala de la Unión y por países, deben reflejar los últimos avances y quedar a cargo del Centro Común de Investigación en colaboración con el INTCEN del SEAE; subraya la necesidad de recursos suficientes para que estas instituciones proporcionen los análisis más avanzados, con una sólida supervisión democrática, lo que no debe excluir una evaluación previa rigurosa por la FRA para garantizar el respeto de los derechos fundamentales;

77. Cree que la Unión y sus Estados miembros deben proporcionar alternativas de financiación a los países candidatos de los Balcanes Occidentales y otros países candidatos potenciales en los que terceros países han utilizado la IED como herramienta geopolítica para aumentar su influencia, para evitar de este modo que una gran parte de sus infraestructuras críticas pase a ser propiedad de países y empresas de fuera de la Unión, como en el caso del puerto del Pireo en Grecia y como está ocurriendo actualmente con las inversiones chinas en cables submarinos en los mares Báltico, Mediterráneo y Ártico; acoge con satisfacción, por consiguiente, el Reglamento para el control de las IED como un instrumento importante para coordinar las acciones de los Estados miembros en materia de inversiones extranjeras, y aboga por un marco regulador más sólido y una garantía más sólida de su cumplimiento para garantizar que se bloqueen las IED que afecten a la seguridad de la Unión, conforme a lo especificado en el Reglamento, y por que se transfieran más competencias de control de las IED a las instituciones de la Unión; pide la abolición del principio de adjudicación a la oferta más baja en las decisiones gubernamentales en materia de inversión; pide a todos los Estados miembros sin mecanismos nacionales de control de las inversiones que adopten dichas medidas; cree que dicho marco debería mejorar su conexión con los análisis independientes llevados a cabo por institutos nacionales y de la Unión u otras partes interesadas pertinentes, como grupos de reflexión, para cartografiar y analizar los flujos de IED; considera que también podría resultar conveniente incluir otros sectores estratégicos en el marco, como el de la red 5G y otras tecnologías de la información y la comunicación (TIC), para limitar la dependencia de la Unión y sus Estados miembros respecto de proveedores de alto riesgo; subraya que este enfoque debe aplicarse igualmente a países candidatos y candidatos potenciales;

78. Cree que la Unión se enfrenta a más retos como resultado de su falta de inversiones en el pasado, que ha contribuido a su dependencia de proveedores de tecnología extranjeros; recomienda blindar las cadenas de producción y de suministro de infraestructuras críticas y materiales críticos en la Unión; considera que el avance de la Unión hacia la autonomía estratégica abierta y la soberanía digital es importante y constituye el camino correcto a seguir; destaca que se espera que la Unión despliegue nuevas herramientas para reforzar su posición geopolítica, incluido un instrumento contra las acciones coercitivas; considera asimismo que la Ley europea de productos semiconductores anunciada por la Comisión para garantizar que se fabriquen en la Unión componentes que son vitales para la producción de chips supone un paso importante para limitar la dependencia respecto de terceros países como China y los Estados Unidos; cree que la inversión en la producción de chips debe hacerse de manera coordinada en toda la Unión y basándose en el lado de la demanda, a fin de evitar una

carrera hacia las subvenciones públicas nacionales y la fragmentación del mercado único; pide, por tanto, a la Comisión que cree un fondo europeo dedicado específicamente a los semiconductores, que podría apoyar la creación de la tan necesaria mano de obra cualificada y compensar los mayores costes de establecimiento de plantas de fabricación y de diseño en la Unión; considera a Taiwán un socio importante para impulsar la producción de semiconductores dentro de la Unión;

79. Pide un mayor desarrollo de las redes europeas de proveedores de infraestructuras y servicios de datos con normas de seguridad europeas, como GAIA-X, como un paso importante hacia el establecimiento de alternativas viables a los actuales proveedores de servicios y hacia una economía digital abierta, transparente y segura; subraya la necesidad de reforzar las pymes y evitar la cartelización del mercado de la nube; recuerda que los centros de datos son infraestructuras críticas; manifiesta su preocupación ante la influencia de terceros países y sus empresas en el desarrollo de GAIA-X;

80. Subraya que la integridad, la disponibilidad y la confidencialidad de las redes de comunicación electrónica públicas, como las redes troncales de internet y los cables de comunicación submarinos, revisten un interés de seguridad vital; pide a la Comisión y a los Estados miembros que impidan el sabotaje y el espionaje en dichas redes de comunicación y que promuevan el uso de normas de encaminamiento seguras e interoperables para garantizar la integridad y la solidez de las redes y servicios de comunicaciones electrónicas, también a través de la reciente estrategia de la «Pasarela Mundial»;

81. Pide a la Comisión que proponga acciones para establecer un suministro seguro y sostenible de las materias primas utilizadas para producir componentes y tecnologías críticos, incluidas pilas y baterías, equipos y tecnologías 5G y subsiguientes, y productos químicos y farmacéuticos, subrayando al mismo tiempo la importancia del comercio mundial, la cooperación internacional con pleno respeto de los derechos de los trabajadores y el entorno natural, y el cumplimiento de las normas sociales y de sostenibilidad internacionales por lo que respecta al uso de los recursos; recuerda la necesidad de conceder la financiación necesaria a la investigación y el desarrollo con el fin de encontrar sustitutos adecuados en caso de perturbación de la cadena de suministro;

***Injerencia extranjera durante los procesos electorales***

82. Pide la protección de todo el proceso electoral como una cuestión prioritaria de seguridad nacional y de la Unión, pues unas elecciones libres y justas constituyen la pieza central del proceso democrático; pide a la Comisión que desarrolle un mejor marco de respuesta para contrarrestar la injerencia extranjera en los procesos electorales, que, entre otras medidas, debe consistir en canales de comunicación directa con los ciudadanos;

83. Destaca la necesidad de fomentar la resiliencia de la sociedad frente a la desinformación durante los procesos electorales, también en los sectores privado y académico, y de adoptar un enfoque holístico en el que dichas injerencias se aborden de forma constante, desde los programas de educación escolar hasta la integridad técnica y la fiabilidad del

voto, y a través de medidas estructurales para hacer frente a su naturaleza híbrida; pide, en particular, un plan para preparar las elecciones europeas de 2024 que incluya una estrategia, formación y sensibilización para los partidos políticos europeos y su personal y medidas de seguridad reforzadas para prevenir las injerencias extranjeras;

84. Considera que la información errónea y la desinformación a través de las redes sociales se han convertido en un problema de gravedad creciente para la integridad electoral; considera que las plataformas de redes sociales deben garantizar la ejecución y el buen funcionamiento de medidas para proteger la integridad de las elecciones; se muestra alarmado por las recientes constataciones relativas a empresas privadas contratadas por agentes malintencionados para interferir en elecciones, diseminar relatos falsos e impulsar conspiraciones virales, sobre todo en las redes sociales; pide una investigación en profundidad sobre cómo contrarrestar el fenómeno de la «desinformación por contrato», ya que se está volviendo cada vez más sofisticado y más común en todo el mundo;

85. Destaca la gran importancia de las misiones de observación electoral a la hora de proporcionar información pertinente y formular recomendaciones específicas para aumentar la resiliencia del sistema electoral y ayudar a contrarrestar las injerencias extranjeras en los procesos electorales; pide que se mejoren y refuercen los procesos electorales y considera las misiones de observación electoral como un instrumento clave para combatir el creciente recurso a procesos electorales injustos y fraudulentos por parte de regímenes iliberales que buscan una apariencia democrática; recalca, en este contexto, la necesidad de reevaluar y actualizar las herramientas y los métodos de la observación electoral internacional para hacer frente a nuevas tendencias y amenazas, incluidos la lucha contra los falsos observadores electorales, el intercambio de mejores prácticas con socios afines y una colaboración más estrecha con las organizaciones internacionales pertinentes, como la Organización para la Seguridad y la Cooperación en Europa (OSCE) y el Consejo de Europa, y todos los agentes pertinentes en el marco de la Declaración de Principios para la Observación Internacional de Elecciones y el Código de Conducta para observadores internacionales de elecciones; destaca que la participación de diputados al Parlamento Europeo en misiones de observación electoral no autorizadas es perjudicial para la credibilidad y la reputación del Parlamento Europeo; acoge con satisfacción y recomienda la plena aplicación del procedimiento del Grupo de Apoyo a la Democracia y Coordinación Electoral para los casos de observación individual no oficial de elecciones por parte de diputados al Parlamento Europeo (aprobado el 13 de diciembre de 2018), que permite la exclusión de diputados al Parlamento Europeo de las delegaciones oficiales de observación electoral del Parlamento por el resto de su mandato;

***Financiación encubierta de actividades políticas por donantes extranjeros***

86. Subraya que, si bien sigue siendo necesaria una mejor comprensión de los efectos de la financiación encubierta de actividades políticas en las tendencias antidemocráticas en Europa, por ejemplo, la financiación extranjera de actividades políticas mediante operaciones encubiertas constituye, no obstante, una grave violación de la integridad del funcionamiento democrático de la Unión y sus Estados miembros, en particular en períodos electorales, y por tanto conculca el principio de unas elecciones libres y justas; destaca que debe declararse ilegal en todos los Estados miembros de la Unión el

ejercicio de toda actividad encubierta financiada por una potencia extranjera que pretenda influir en procesos políticos europeos o nacionales; observa, a este respecto, que países como Australia han adoptado leyes que prohíben la injerencia extranjera en la política;

87. Condena el hecho de que partidos extremistas, populistas, antieuropeos y otros partidos e individuos estén relacionados con intentos de interferir en los procesos democráticos de la Unión y son cómplices explícitos en ellos, y expresa su alarma ante el hecho de que estos partidos sean utilizados como portavoces de agentes de injerencias extranjeras para legitimar a sus gobiernos autoritarios; pide la plena aclaración de las relaciones políticas y económicas entre estos partidos e individuos y Rusia; considera que estas relaciones son muy inapropiadas y condena la complicidad que, en pos de objetivos políticos, puede exponer a la Unión y a sus Estados miembros a ataques de potencias extranjeras;

88. Pide a los Estados miembros que, cuando profundicen en la armonización de las normativas nacionales, subsanen todas las lagunas siguientes, y que prohíban las donaciones extranjeras:

a) contribuciones en especie de agentes extranjeros a partidos políticos, fundaciones, personas que ocupan cargos públicos o cargos electos, incluidos los préstamos financieros de cualquier persona física o jurídica establecida fuera de la Unión y del Espacio Económico Europeo (EEE) (excepto los votantes europeos), donaciones anónimas por encima de un determinado umbral, y la ausencia de límites de gasto en campañas políticas, que permite que se ejerza influencia a través de grandes donaciones; debe obligarse a los responsables, agentes o partidos políticos a los que se haya ofrecido o que hayan aceptado una contribución financiera o en especie por un agente extranjero a notificarlo a las autoridades competentes, y esta información debe comunicarse a nivel de la Unión para hacer posible su seguimiento en toda la Unión;

b) las donaciones mediante testaferros con ciudadanía nacional[17]: debe velarse por la transparencia respecto a los donantes físicos y jurídicos mediante declaraciones de conformidad que acrediten la condición de donante, y otorgando a las comisiones electorales mayores facultades para velar por el cumplimiento de la legislación; las donaciones procedentes del interior de la Unión que excedan de un determinado umbral mínimo deben registrarse en un registro oficial y vincularse a una persona física, y debe establecerse un límite máximo para las donaciones de personas particulares y jurídicas (y subvenciones) a partidos políticos;

c) las sociedades ficticias y filiales nacionales de sociedades matrices extranjeras[18]: las sociedades ficticias deben prohibirse y han de establecerse requisitos más sólidos respecto a la revelación de los orígenes de la financiación a través de sociedades matrices; la financiación y las donaciones a partidos políticos más allá

[17] Personas que donan en su propio nombre el dinero de un tercero a un partido o candidato político.
[18] Esta laguna encubre dos realidades diferentes: las sociedades fantasma, que no desempeñan actividades empresariales reales y no son nada más que una tapadera para encubrir fuentes de financiación, y las filiales nacionales de empresas matrices, que se usan para canalizar fondos a la política.

de un determinado umbral deben registrarse en un registro público central con un nombre y una dirección oficiales que puedan vincularse a una persona existente, y los Estados miembros deben recopilar dicha información; pide a la Comisión que garantice que las autoridades de los Estados miembros tengan derecho a investigar los orígenes de la financiación para verificar la información de las filiales nacionales y abordar la falta de datos suficientes en los registros nacionales, especialmente en situaciones en las que se utilice una red de sociedades ficticias;

d) organizaciones sin ánimo de lucro y terceros[19], coordinados por agentes extranjeros y creados con la intención de influir en los procesos electorales: debe considerarse la adopción de normas más uniformes y el fomento de la transparencia en toda la Unión respecto a las organizaciones que deseen financiar actividades políticas cuando traten de influir directamente en procesos electorales como las elecciones y las campañas de referéndums; dichas normas no deben impedir a los terceros y organizaciones sin ánimo de lucro recibir financiación para campañas temáticas; las normas que garanticen la transparencia de la financiación o las donaciones también deben aplicarse a las fundaciones políticas;

e) los anuncios políticos en línea, que no están sujetos a las normas sobre publicidad en televisión, radio y prensa escrita y, habitualmente, no se someten a ningún tipo de regulación: por lo tanto, es necesario prohibir los anuncios comprados por agentes procedentes de fuera de la Unión y del EEE y garantizar la plena transparencia en cuanto a la compra de publicidad política en línea por agentes del interior de la Unión; subraya la necesidad de garantizar una transparencia y una responsabilidad democrática muy superiores en lo que atañe al uso de algoritmos; acoge con satisfacción el anuncio de la presentación por la Comisión de una nueva propuesta legislativa sobre la transparencia de los contenidos políticos patrocinados, tal como se propone en el Plan de Acción para la Democracia Europea, que debe tener por objeto evitar un mosaico de veintisiete legislaciones nacionales distintas en materia de publicidad política en línea y garantizará que los partidos políticos de la Unión puedan hacer campaña en línea antes de las elecciones europeas, limitando asimismo el riesgo de injerencia extranjera y estudiando cuáles de las normas adoptadas voluntariamente por los partidos políticos de cada Estado miembro y por las principales plataformas de redes sociales pueden convertirse en normas para todos en la Unión; pide a los Estados miembros de la Unión que actualicen sus normativas nacionales sobre publicidad política, que no han seguido el ritmo de la evolución constante hacia el medio digital como modalidad principal de comunicación política; pide a la Comisión que proponga cómo definir democráticamente la publicidad política temática para poner fin a una situación en que las plataformas privadas con ánimo de lucro deciden lo que es temático y lo que no lo es;

f) debe establecerse un control del gasto electoral a través de auditores independientes y garantizarse que la información sobre gastos y donaciones esté disponible oportunamente para auditores independientes, mitigando así riesgos

[19] Las organizaciones sin ánimo de lucro y los terceros no están obligados a revelar la identidad de sus donantes, pero pueden financiar a partidos políticos y candidatos en varios Estados miembros de la Unión.

como los conflictos de intereses y las presiones en relación con la financiación política; a la hora de establecer una divulgación proactiva, las instituciones responsables de las regulaciones financieras deben contar con un mandato claro, la capacidad, los recursos y el poder jurídico para llevar a cabo investigaciones y remitir casos para su enjuiciamiento;

89. Pide, por tanto, a la Comisión que realice un análisis de la financiación encubierta en la Unión y que presente propuestas concretas destinadas a colmar todas las lagunas que permiten la financiación opaca de partidos políticos y fundaciones políticas o cargos electos por parte de terceros países y que proponga unas normas comunes de la Unión que se apliquen a la legislación electoral nacional en todos los Estados miembros; considera que los Estados miembros deben introducir requisitos claros de transparencia en relación con la financiación de los partidos políticos, así como la prohibición de las donaciones a partidos políticos y agentes políticos individuales procedentes de fuera de la Unión y el EEE, con la excepción de los votantes europeos que residen fuera de la Unión y el EEE, y establecer una estrategia clara respecto al sistema de sanciones; insta a la Comisión y a los Estados miembros a que establezcan una autoridad de la Unión para los controles financieros con el fin de combatir las prácticas financieras ilícitas y la injerencia de Rusia y otros regímenes autoritarios; destaca la necesidad de prohibir las donaciones o financiación que utilicen tecnologías emergentes de muy difícil trazabilidad; pide a los Estados miembros y a la Comisión que asignen más recursos y mandatos más sólidos a las agencias de supervisión con vistas a lograr una mejor calidad de los datos;

90. Se compromete a garantizar que todas las organizaciones sin ánimo de lucro, los grupos de reflexión, los institutos y las ONG que contribuyan a la labor parlamentaria para el desarrollo de la política de la Unión o que desempeñen cualquier papel de consulta en el proceso de elaboración legislativa sean plenamente transparentes e independientes y estén libres de conflictos de intereses en términos de su financiación y su titularidad;

91. Acoge favorablemente la revisión en curso del Reglamento (UE, Euratom) n.º 1141/2014 sobre el estatuto y la financiación de los partidos políticos europeos y las fundaciones políticas europeas; apoya todos los esfuerzos encaminados a lograr un mayor nivel de transparencia en la financiación de las actividades de los partidos políticos europeos y las fundaciones políticas europeas, en particular de cara a las elecciones europeas de 2024, incluida la prohibición de todas las donaciones procedentes de fuentes de fuera de la Unión y anónimas, exceptuando la diáspora de los Estados miembros de la Unión, y de las donaciones procedentes de fuera de la Unión que no puedan documentarse mediante un contrato, acuerdos de servicio o cuotas asociadas a la afiliación a un partido político europeo, permitiendo al mismo tiempo las cuotas de adhesión de miembros de partidos nacionales que se encuentren fuera de la Unión y el EEE a partidos políticos europeos; insta a los partidos políticos europeos y nacionales a que se comprometan a luchar contra la injerencia extranjera y a combatir la difusión de desinformación firmando una Carta que contenga compromisos específicos a este respecto;

92. Destaca que la aplicación de muchas de las recomendaciones del GRECO del Consejo de Europa y de la Comisión de Venecia reforzarían la inmunidad del sistema político de los Estados miembros y de la Unión frente a la influencia financiera extranjera;

*Ciberseguridad y resiliencia frente a ciberataques*

93. Insta a las instituciones de la Unión y a los Estados miembros a que aumenten rápidamente las inversiones en las capacidades digitales estratégicas y las aptitudes de la Unión para detectar, exponer y abordar la injerencia extranjera, como la inteligencia artificial, la comunicación segura y la infraestructura de datos y computación en la nube, con el fin de mejorar la ciberseguridad de la Unión, garantizando al mismo tiempo el respeto de los derechos fundamentales; pide a la Comisión que también invierta más en incrementar el conocimiento digital en la Unión y las competencias técnicas especializadas para entender mejor los sistemas digitales utilizados en toda la Unión; pide a la Comisión que asigne recursos humanos, materiales y financieros adicionales a las capacidades de análisis de ciberamenazas, concretamente el INTCEN del SEAE, y la ciberseguridad de las instituciones, órganos y organismos de la Unión, concretamente ENISA y el Equipo de Respuesta a Emergencias Informáticas de las instituciones de la UE (CERT-UE), y los Estados miembros; lamenta la falta de cooperación y armonización en materia de ciberseguridad entre los Estados miembros;

94. Acoge con satisfacción las propuestas de la Comisión relativas a una nueva estrategia de ciberseguridad y una nueva Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión Europea, por la que se deroga la Directiva (UE) 2016/1148[20] (SRI 2); recomienda que el resultado final de los trabajos en curso sobre la propuesta aborde las deficiencias de la Directiva SRI de 2016, en particular mediante el refuerzo de los requisitos de seguridad, la ampliación del ámbito, la creación de un marco para la cooperación y el intercambio de información europeos, el refuerzo de las capacidades de ciberseguridad de los Estados miembros, el desarrollo de la cooperación público-privada, la introducción de requisitos de ejecución más estrictos y la consolidación de la ciberseguridad como responsabilidad para el nivel más alto de dirección de las entidades europeas que son fundamentales para nuestra sociedad; subraya la importancia de alcanzar un elevado nivel común de ciberseguridad en todos los Estados miembros para limitar las deficiencias en la ciberseguridad conjunta de la Unión; subraya la necesidad crucial de garantizar la resiliencia de los sistemas de información y acoge con satisfacción, a este respecto, la Red de organizaciones de enlace para crisis cibernéticas (CyCLONe); alienta a que se sigan promoviendo medidas de desarrollo de la confianza de la OSCE para el ciberespacio;

95. Acoge favorablemente la propuesta de la Comisión en la Directiva SRI 2 de llevar a cabo evaluaciones de riesgos de seguridad coordinadas de las cadenas de suministro críticas, análogas al conjunto de herramientas de la Unión sobre 5G, con el fin de tener más en cuenta los riesgos vinculados, por ejemplo, al uso de *software* y *hardware* producidos por empresas bajo el control de Estados autoritarios extranjeros; pide a la Comisión que elabore estándares y normas de competencia de escala mundial sobre 6G, de conformidad con los valores democráticos; pide asimismo a la Comisión que promueva intercambios entre las instituciones de la Unión y las autoridades nacionales sobre los retos, las buenas prácticas y las soluciones relacionados con las medidas del conjunto de instrumentos; cree que la Unión debe invertir más en sus capacidades en el

[20] Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148, COM(2020)0823.

ámbito de las tecnologías 5G y post-5G, con el fin de reducir la dependencia respecto a proveedores extranjeros;

96. Destaca que la ciberdelincuencia no conoce fronteras e insta a la Unión a que redoble sus esfuerzos internacionales para hacerle frente de manera eficaz; señala que la Unión debe asumir el liderazgo en el desarrollo de un Tratado Internacional sobre Ciberseguridad que establezca normas internacionales sobre ciberseguridad para luchar contra la ciberdelincuencia;

97. Acoge con satisfacción el anuncio de la elaboración de una ley de ciberresiliencia que complemente la política europea de ciberdefensa, ya que el ámbito cibernético y el de la defensa están estrechamente relacionados; pide más inversiones en capacidades y coordinación europeas en materia de ciberdefensa; recomienda que se fomente el desarrollo de cibercapacidades entre nuestros socios a través de misiones de formación de la Unión o cibermisiones civiles; subraya la necesidad de armonizar y normalizar la formación relacionada con el ciberespacio y pide financiación estructural de la Unión en este ámbito;

98. Condena el uso ilícito y a gran escala del *software* de vigilancia y programa espía Pegasus del grupo NSO por parte de entidades estatales, como Marruecos, Arabia Saudí, Hungría, Polonia, Baréin, los Emiratos Árabes Unidos y Azerbaiyán, contra periodistas, defensores de los derechos humanos y políticos; recuerda que Pegasus es solo uno de los muchos casos de programas utilizados indebidamente por entidades estatales para fines de vigilancia masiva ilícita contra ciudadanos inocentes; condena asimismo otras operaciones estatales de espionaje dirigidas contra políticos europeos; insta a la Comisión a que elabore una lista de programas informáticos de vigilancia ilícitos y a que la actualice continuamente; pide a la Unión y a los Estados miembros que utilicen esta lista para garantizar la plena diligencia debida en materia de derechos humanos y un examen adecuado de las exportaciones de tecnología y asistencia técnica de vigilancia europeas y de las importaciones a los Estados miembros que planteen riesgos claros para el Estado de Derecho; pide, además, la creación de un laboratorio de ciudadanos de la Unión similar al establecido en Canadá, compuesto por periodistas, expertos en derechos humanos y expertos en ingeniería inversa de programas malintencionados, que trabajaría para descubrir y exponer el uso ilegal de programas informáticos con fines de vigilancia ilícita;

99. Pide a la Unión que adopte un marco regulador sólido en este ámbito a nivel de la Unión y a nivel internacional; acoge favorablemente, a este respecto, la decisión de la Oficina de Industria y Seguridad del Departamento de Comercio de Estados Unidos de incluir en una lista negra al grupo NSO Technologies, prohibiendo con ello que la empresa reciba tecnologías estadounidenses;

100. Manifiesta su preocupación al observar que la Unión está cooperando en asuntos judiciales y policiales con terceros países con relaciones con el grupo NSO y que han utilizado el programa espía Pegasus para espiar a ciudadanos de la Unión; pide salvaguardas adicionales y un control democrático reforzado de dicha cooperación;

101. Pide a la Comisión que examine las inversiones europeas en el grupo NSO Technologies y que adopte medidas específicas contra los Estados extranjeros que

utilicen programas para espiar a ciudadanos de la Unión o a personas que se beneficien del estatuto de refugiado en países europeos;

102. Expresa su preocupación por que periodistas y activistas de la democracia puedan ser objeto de actividades de vigilancia ilegales y de acoso por parte de los regímenes autoritarios de los que pretenden escapar, incluso en suelo de la Unión, y considera que este tipo de actuaciones supone una grave violación de los valores fundamentales de la Unión y de los derechos fundamentales de las personas, tal como se establece en la Carta de los Derechos Fundamentales, el Convenio Europeo de Derechos Humanos (CEDH) y el Pacto Internacional de Derechos Civiles y Políticos; lamenta la falta de asistencia jurídica prestada a las víctimas de este *software* espía;

103. Destaca la necesidad urgente de reforzar el marco legislativo para exigir responsabilidades a quienes distribuyan y utilicen abusivamente dicho *software* con fines ilícitos y no autorizados; se refiere, en particular, a las sanciones impuestas el 21 de junio de 2021 a Alexander Shatrov, primer ejecutivo de una empresa bielorrusa que produce *software* de reconocimiento facial utilizado por un régimen autoritario, por ejemplo para identificar a manifestantes de la oposición política; pide a la Comisión que impida cualquier uso o financiación en la Unión de tecnologías de vigilancia ilegales; pide a la Unión y a los Estados miembros que colaboren con Gobiernos de terceros países para poner fin a las prácticas represivas y la legislación en materia de ciberseguridad y de lucha contra el terrorismo, con un control democrático reforzado; pide una investigación por parte de las autoridades competentes de la Unión sobre el uso ilícito de programas espía en la Unión y las exportaciones de tales programas desde la Unión, y que haya repercusiones para los Estados miembros y los Estados asociados que hayan comprado y utilizado programas espía y que los hayan exportado para espiar ilegalmente a periodistas, defensores de los derechos humanos, abogados y políticos;

104. Aboga por una revisión ambiciosa de la Directiva sobre la privacidad y las comunicaciones electrónicas[21], con el fin de reforzar la confidencialidad de las comunicaciones y los datos personales al utilizar dispositivos electrónicos, sin reducir el nivel de protección que proporciona la Directiva y sin perjuicio de la responsabilidad de los Estados miembros de salvaguardar la seguridad nacional; destaca que debería obligarse a las autoridades públicas a divulgar las vulnerabilidades que detecten en dispositivos de TI; pide a la Unión y a los Estados miembros que sigan coordinando sus acciones con arreglo a la Directiva relativa a los ataques contra los sistemas de información[22], con el fin de garantizar que el acceso ilegal a los sistemas de información y la interceptación ilegal se definan como delitos y reciban sanciones adecuadas; recuerda que toda violación de la confidencialidad con fines de seguridad nacional debe llevarse a cabo legalmente y con fines explícitos y legítimos en una sociedad democrática, con arreglo a los principios de estricta necesidad y proporcionalidad,

[21] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (DO L 201 de 31.7.2002, p. 37).
[22] Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión Marco 2005/222/JAI del Consejo (DO L 218 de 14.8.2013, p. 8).

conforme a las exigencias del CEDH y el Tribunal de Justicia de la Unión Europea;

***Protección de los Estados miembros, instituciones, agencias, delegaciones y misiones de la Unión***

105. Subraya que las redes, los edificios y el personal de las instituciones, las agencias, los organismos, las delegaciones y las misiones y operaciones de la Unión representan un objetivo para todo tipo de amenazas y ataques híbridos por parte de agentes de Estados extranjeros y, por tanto, deben protegerse debidamente, y que debe prestarse una especial atención a la seguridad de los bienes, los locales y las actividades del SEAE en el extranjero y a la seguridad del personal de la Unión delegado en países no democráticos con regímenes represivos; pide una respuesta estructurada a estas amenazas por parte de las misiones de la PCSD, así como un apoyo más concreto a dichas misiones a través de la comunicación estratégica; toma nota del aumento constante de los ataques patrocinados por Estados contra instituciones, órganos y agencias de la Unión, incluida la EMA, instituciones de los Estados miembros y autoridades públicas nacionales;

106. Pide una revisión exhaustiva y periódica de todos los servicios, redes, equipos y *hardware* de las instituciones, órganos, agencias, delegaciones, misiones y operaciones de la Unión con el fin de reforzar su resiliencia frente a las amenazas de ciberseguridad y excluir programas y dispositivos potencialmente peligrosos, como los desarrollados por Kaspersky Lab; insta a las instituciones de la Unión y a los Estados miembros a garantizar la provisión de orientaciones adecuadas y herramientas seguras al personal; hace hincapié en la necesidad de fomentar la sensibilización respecto al uso de servicios y redes seguros en las instituciones y las administraciones, también durante las misiones; observa la fiabilidad y las ventajas de seguridad de los sistemas operativos de red basados en código abierto, ampliamente utilizado por agencias militares y gubernamentales aliadas;

107. Subraya la importancia de una coordinación eficiente, oportuna y estrecha entre las diferentes instituciones, órganos y agencias de la Unión especializados en ciberseguridad, como el CERT-UE, junto con el pleno desarrollo de sus capacidades operativas, así como la ENISA y la futura unidad informática conjunta, que garantizarán una respuesta coordinada a las amenazas a la ciberseguridad a gran escala en la Unión; acoge favorablemente la cooperación estructurada en curso entre el CERT-UE y la ENISA; acoge con satisfacción, asimismo, el establecimiento de un grupo de trabajo de ciberinteligencia de la Unión en el seno del INTCEN de la UE con vistas a avanzar en la cooperación en materia de inteligencia estratégica; valora positivamente las recientes iniciativas emprendidas por los secretarios generales de las instituciones de la Unión para desarrollar normas comunes de información y ciberseguridad;

108. Espera con interés las dos propuestas de Reglamento de la Comisión por las que se establece un marco normativo para la seguridad de la información y la ciberseguridad en todas las instituciones, órganos y agencias de la Unión, y considera que estos reglamentos deben incluir el refuerzo de capacidades y de la resiliencia; pide a la Comisión y a los Estados miembros que asignen fondos y recursos adicionales a la ciberseguridad de las instituciones de la Unión para hacer frente a los retos de un panorama de amenazas en constante evolución;

109. Espera asimismo con interés el Informe especial sobre la auditoría de la ciberseguridad del Tribunal de Cuentas Europeo, previsto para principios de 2022;

110. Pide una investigación exhaustiva de los casos denunciados de infiltración extranjera entre el personal de las instituciones de la Unión; pide un examen y una posible revisión de los procedimientos de recursos humanos, incluido el control previo a la contratación, para colmar las lagunas que permiten la infiltración extranjera; pide a los órganos de gobierno del Parlamento que mejoren los procedimientos de habilitación de seguridad del personal y que endurezcan las normas y los controles para el acceso a sus locales, a fin de evitar que personas estrechamente vinculadas a intereses extranjeros tengan acceso a reuniones e información confidenciales; pide a las autoridades belgas que revisen y actualicen su marco nacional contra el espionaje para hacer posible la detección, el enjuiciamiento y la penalización eficaces de los infractores; pide que se lleven a cabo acciones similares en los demás Estados miembros para proteger a las instituciones y agencias de la Unión establecidas en su territorio;

111. Insta a todas las instituciones de la Unión a sensibilizar a su personal mediante la formación y la orientación adecuadas para prevenir, mitigar y abordar los riesgos de seguridad cibernética y no cibernética; pide que se imparta formación obligatoria y periódica sobre seguridad a todo el personal (también los becarios) y a los diputados al PE; pide una cartografía y una evaluación periódicas y específicas del riesgo de influencia extranjera en el seno de las instituciones;

112. Subraya la necesidad de procedimientos de gestión de crisis adecuados para los casos de manipulación de la información, incluidos los sistemas de alerta entre niveles administrativos y sectores, con el fin de garantizar el suministro de información mutua y evitar la propagación de la manipulación de la información; acoge con satisfacción, en este sentido, el sistema de alerta rápida (SAR) y el procedimiento de alerta rápida establecidos antes de las elecciones europeas de 2019, así como los procedimientos aplicados en las administraciones de la Comisión y del Parlamento para advertir de posibles casos que afecten a las instituciones o a los procesos democráticos de la Unión; pide a la administración de la Unión que refuerce su supervisión, también a través del establecimiento de un repositorio central y de una herramienta de rastreo de incidentes, y que desarrolle una instrumental compartido para su activación en caso de alerta del SAR;

113. Pide normas de transparencia obligatorias para los viajes ofrecidos por países y entidades extranjeros a funcionarios de las instituciones de la Unión, así como a diputados al Parlamento Europeo, asistentes parlamentarios acreditados y asesores de grupo, y también a funcionarios nacionales, en cuanto a los datos siguientes (sin ánimo de exhaustividad): el nombre de los agentes pagadores, el importe de los viajes y los motivos declarados; recuerda que dichos viajes organizados no pueden considerarse delegaciones oficiales del Parlamento y pide sanciones estrictas en caso de que esto no se respete; hace hincapié en que los grupos de amistad informales pueden contrarrestar el trabajo de los organismos oficiales del Parlamento, así como menoscabar su reputación y la coherencia de sus acciones; insta a los órganos de gobierno del Parlamento a que aumenten la transparencia y la rendición de cuentas de estos grupos, a que velen por el respeto de la normativa vigente y a que adopten las medidas necesarias cuando terceros países hagan un uso indebido de estos grupos de amistad; pide a los

Cuestores que desarrollen y mantengan un registro accesible y actualizado de los grupos de amistad y las declaraciones;

***Injerencia por medio de agentes globales a través de la captación de élites, las diásporas nacionales, universidades y actos culturales***

114. Condena todo tipo de captación de élites, así como la técnica de cooptación de funcionarios de alto nivel y antiguos políticos de la Unión empleada por empresas extranjeras con vínculos con Gobiernos que desarrollan actividades de injerencia contra la Unión, y lamenta la ausencia de los instrumentos y las medidas coercitivas necesarios para impedir estas prácticas; considera que la revelación, en detrimento de los intereses estratégicos de la Unión y de sus Estados miembros, de información confidencial obtenida durante el ejercicio de mandatos públicos o en el desempeño de funciones públicas debe tener consecuencias jurídicas y ser objeto de sanciones severas, como la destitución inmediata y la inhabilitación para futuras contrataciones por las instituciones; considera que deben hacerse públicas las declaraciones de la renta y del patrimonio de estas personas;

115. Pide a la Comisión que fomente y coordine acciones contra la captación de élites, como complementar y aplicar sin excepciones los períodos de incompatibilidad de los comisarios de la UE y los funcionarios europeos de alto nivel con una obligación de información una vez concluidos períodos, con vistas a poner fin a la práctica de las «puertas giratorias» y normas estructuradas para hacer frente a la captación de élites a escala de la Unión; pide a la Comisión que evalúe si las obligaciones actuales en materia de incompatibilidad siguen siendo adecuados para su propósito; destaca que los antiguos políticos y funcionarios de la Unión deben informar a un órgano de supervisión específico cuando sean abordados por un Estado extranjero y, en ese caso, gozar de la protección de los denunciantes; pide a todos los Estados miembros que apliquen y armonicen los períodos de incompatibilidad para sus dirigentes políticos y que velen por la existencia de medidas y sistemas que obliguen a los funcionarios públicos a declarar sus actividades exteriores, empleos, inversiones, activos y obsequios o beneficios sustanciales de los que pueda derivarse un conflicto de intereses;

116. Considera con preocupación las estrategias integradas de los grupos de presión que combinan intereses industriales y objetivos políticos extranjeros, en particular cuando favorecen los intereses de un Estado autoritario; pide, por tanto, a las instituciones de la Unión que reformen el Registro de transparencia, entre otras vías, mediante la adopción de normas de transparencia más estrictas, la determinación de cómo se asignan los fondos extranjeros a las actividades de representación de intereses relacionadas con la Unión, y la garantía de una inscripción en el Registro que permita la identificación de fondos procedentes de Gobiernos extranjeros; pide una cooperación eficaz a este respecto entre todas las instituciones de la Unión; considera que el programa australiano sobre transparencia de la influencia extranjera constituye una buena práctica a seguir;

117. Pide a los Estados miembros que consideren el establecimiento de un sistema de registro de influencias extranjeras y la creación de un registro gestionado por la administración pública de actividades declaradas emprendidas para un Estado extranjero o en nombre de este, siguiendo las buenas prácticas de otras democracias de ideas afines;

118. Expresa su preocupación por los intentos de control de las diásporas que residen en suelo de la Unión por parte de Estados autoritarios extranjeros; destaca el papel crucial desempeñado por el Frente Unido de China, que es un departamento que depende directamente del Comité Central del Partido Comunista de China y se encarga de coordinar la estrategia de injerencia exterior de este país a través del estricto control de los ciudadanos chinos y las empresas chinas en el extranjero; destaca asimismo las experiencias de Australia y Nueva Zelanda en su tratamiento del Frente Unido;

119. Condena enérgicamente los esfuerzos del Kremlin por servirse de minorías presentes en Estados miembros de la Unión aplicando las denominadas «políticas compatriotas», en particular en los Estados bálticos y los países de la Vecindad Oriental, como parte de la estrategia geopolítica del régimen de Putin, cuyo objetivo es dividir las sociedades de la Unión, junto con la aplicación del concepto de «mundo ruso», encaminado a justificar las actividades expansionistas del régimen; señala que muchas «fundaciones privadas», «empresas privadas», «medios de comunicación» y «ONG» rusos o bien son propiedad del Estado, o bien mantienen vínculos ocultos con el Estado ruso a través de estructuras complejas, o bien dependen de la financiación estatal; destaca que, en el marco del diálogo con la sociedad civil rusa, es de la máxima importancia diferenciar entre las organizaciones que se mantienen alejadas de la influencia gubernamental rusa y las que mantienen vínculos con el Kremlin; recuerda que existen también pruebas de injerencia y manipulación rusas en muchas otras democracias liberales occidentales, así como del apoyo activo a fuerzas extremistas y entidades de pensamiento radical para promover la desestabilización de la Unión; señala que el Kremlin hace un amplio uso de la cultura como arma, incluidos la música popular, los contenidos audiovisuales y la literatura, como parte de su ecosistema de desinformación; lamenta los intentos de Rusia de no reconocer plenamente la historia de los crímenes soviéticos y, en su lugar, de introducir una nueva narrativa rusa;

120. Manifiesta su preocupación por los intentos del Gobierno turco de influir en personas con raíces turcas con el objetivo de utilizar la diáspora como retransmisor de las posiciones de Ankara y dividir las sociedades europeas, en particular a través de la Presidencia de Turcos en el Extranjero y Comunidades Relacionadas (YTB, por sus siglas en turco); condena los intentos manifiestos de Turquía de utilizar su diáspora en Europa para modificar el curso de elecciones;

121. Condena los esfuerzos de Rusia por explotar las tensiones étnicas en los Balcanes Occidentales para atizar conflictos y dividir comunidades, lo que podría conducir a la desestabilización de la región en su conjunto; manifiesta su preocupación ante las tentativas de la Iglesia ortodoxa en países como Serbia, Montenegro y Bosnia y Herzegovina, especialmente en su entidad Republika Srpska, para promover a Rusia como protectora de los valores familiares tradicionales y para reforzar las relaciones entre Estado e Iglesia; expresa su alarma al observar que países como Hungría y Serbia están ayudando a China y Rusia con sus objetivos geopolíticos; recomienda que se convoquen diálogos con la sociedad civil de los Balcanes Occidentales y el sector privado para coordinar los esfuerzos dirigidos a combatir la desinformación en la región, haciendo hincapié en la investigación y el análisis y en la inclusión de los conocimientos especializados regionales; pide a la Comisión que desarrolle las infraestructuras necesarias para crear respuestas basadas en datos a las amenazas de desinformación a corto y largo plazo en los Balcanes Occidentales; pide al SEAE que

adopte una actitud más proactiva, centrándose en mejorar la credibilidad de la Unión en la región, en vez de defenderla, y ampliando la supervisión de la división StratCom para centrarla en las amenazas de desinformación transfronterizas procedentes de países de los Balcanes Occidentales y su vecindad;

122. Resalta la necesidad de que la Unión y sus Estados miembros incrementen su apoyo a los países de la Asociación Oriental, en particular a través de la cooperación para mejorar la resiliencia del Estado y la sociedad frente a la desinformación y la propaganda estatal rusa, a fin de combatir el debilitamiento y la fragmentación estratégicos de sus sociedades e instituciones;

123. Expresa su alarma ante la aplicación extraterritorial de medidas coercitivas derivadas de la nueva Ley de seguridad nacional de Hong Kong y de la Ley china de lucha contra las sanciones internacionales, junto con los acuerdos de extradición de los que China disfruta con otros países, lo que le permite ejecutar acciones de disuasión a gran escala contra ciudadanos críticos no chinos, por ejemplo, en un caso reciente, contra dos parlamentarios daneses, así como las contrasanciones chinas a cinco diputados al Parlamento Europeo, la Subcomisión de Derechos Humanos del Parlamento, tres parlamentarios de Estados miembros de la Unión, el Comité Político y de Seguridad del Consejo, dos académicos europeos y dos grupos de reflexión europeos de Alemania y Dinamarca; pide a los Estados miembros que resistan y rehúsen la extradición y, cuando proceda, brinden una protección adecuada a las personas afectadas para evitar posibles violaciones de los derechos humanos;

124. Considera con preocupación el número de universidades, escuelas y centros culturales europeos que participan en asociaciones con entidades chinas, incluidos los institutos Confucio, que propician el robo de conocimientos científicos y el ejercicio de un control estricto sobre todos los temas relacionados con China en el ámbito de la investigación y la enseñanza, lo que constituye una violación de la protección constitucional de la libertad y la autonomía académicas, y sobre las opciones de las actividades culturales relacionadas con China; manifiesta su preocupación por que tales acciones puedan dar lugar a una pérdida de conocimientos sobre las cuestiones relacionadas con China, lo que privaría a la Unión de las competencias necesarias; expresa su inquietud, por ejemplo, ante el patrocinio, en 2014, de la Biblioteca de China del Colegio de Europa por la Oficina de Información del Consejo de Estado del Gobierno chino[23]; manifiesta su profunda preocupación ante las tentativas de China de ejercer presión e imponer censuras, por ejemplo al museo de Nantes a causa de la exposición sobre Genghis Kahn, inicialmente prevista para 2020[24]; pide a la Comisión que facilite el intercambio de buenas prácticas entre los Estados miembros con el fin de combatir la injerencia extranjera en los sectores de la cultura y la educación;

125. Expresa su preocupación ante los casos de financiación encubierta de investigaciones llevadas a cabo en Europa, incluidos los intentos de China de sustracción de talentos a través del Plan de los Mil Talentos y las becas del Instituto Confucio, así como la mezcla deliberada de proyectos científicos militares y civiles a través de la estrategia china de fusión de los ámbitos civil y militar; resalta los intentos de instituciones de

[23] https://www.coleurope.eu/events/official-inauguration-china-library
[24] https://www.chateaunantes.fr/expositions/fils-du-ciel-et-des-steppes/

enseñanza superior chinas de firmar con instituciones socias de Europa memorandos de entendimiento que contienen cláusulas que perpetúan la propaganda china o fomentan el apoyo a posiciones o iniciativas políticas del Partido Comunista de China, como la iniciativa de la Franja y la Ruta, eludiendo y socavando así las posiciones oficiales adoptadas por los Gobiernos de los países en cuestión; pide a las instituciones culturales, académicas y no gubernamentales que mejoren la transparencia respecto de la influencia de China y que hagan públicos todos los intercambios y colaboraciones con el Gobierno chino y organizaciones relacionadas con este;

126. Condena la decisión adoptada por el Gobierno húngaro de abrir una sucursal de la Universidad de Fudan y, al mismo tiempo, cerrar la Universidad Europea Central de Budapest; considera con preocupación la creciente dependencia financiera de las universidades europeas respecto a China y otros Estados extranjeros, así como el riesgo de que datos, tecnologías y resultados de investigación de carácter sensible fluyan hacia Estados extranjeros y las consecuencias que ello podría tener para la libertad académica; hace hincapié en la importancia de la libertad académica para combatir las operaciones de desinformación e influencia; insta a esas instituciones a que lleven a cabo evaluaciones de la vulnerabilidad detalladas antes de acordar nuevas asociaciones con socios extranjeros; destaca que el personal académico debe recibir formación para informar a través de una línea directa específica sobre casos de financiación encubierta o de influencia y que quienes lo hagan deben beneficiarse siempre la protección concedida a los denunciantes; insta a la Comisión y a los Estados miembros a que garanticen que las investigaciones de trascendencia geopolítica realizadas en las universidades europeas se financien con fondos europeos; pide a la Comisión que proponga legislación para reforzar la transparencia de la financiación extranjera de universidades, así como de ONG y grupos de reflexión, por ejemplo, mediante la declaración obligatoria de las donaciones, la aplicación de la diligencia debida a sus fuentes de financiación y la divulgación de las financiaciones, las contribuciones en especie y las subvenciones de procedencia extranjera; pide a las autoridades de los Estados miembros que adopten normas eficaces en materia de financiación extranjera de las instituciones de enseñanza superior, como requisitos de información y límites máximos estrictos;

127. Destaca que se registran riesgos similares en materia de seguridad y robo de propiedad intelectual en el sector privado, en el que los empleados pueden tener acceso a tecnologías clave y secretos comerciales; pide a la Comisión y a los Estados miembros que alienten a las instituciones académicas y al sector privado a que implanten programas exhaustivos de seguridad y cumplimiento, incluidas revisiones específicas de seguridad para los nuevos contratos; señala que unas mayores limitaciones del acceso a sistemas y redes, así como unas normas más estrictas de habilitación de seguridad, pueden estar justificadas para algunos profesores o empleados cuyo trabajo esté relacionado con investigaciones o productos de vital importancia;

128. Observa que la Directiva sobre la tarjeta azul revisada[25], que facilita la entrada en la Unión a migrantes cualificados nacionales de terceros países, permite, por ejemplo, a

[25] Directiva (UE) 2021/1883 del Parlamento Europeo y del Consejo, de 20 de octubre de 2021, relativa a las condiciones de entrada y residencia de nacionales de terceros países con fines de empleo de alta cualificación, y por el que se deroga la Directiva 2009/50/CE del Consejo (DO L 382 de 28.10.2021, p. 1).

empresas chinas y rusas con sede en Europa invitar a migrantes cualificados de sus respectivos países; señala que esto podría dificultar a los Estados miembros el ejercicio de un control de la afluencia de estos ciudadanos, lo que podría generar riesgos de injerencia extranjera;

129. Expresa su preocupación ante el número creciente de institutos Confucio establecidos en todo el mundo, y en particular en Europa; señala que el Centro para la Educación y la Cooperación Lingüísticas, anteriormente conocido como Oficina Central del Instituto Confucio o Hanban (Oficina del Consejo Internacional de la Lengua China), que es responsable del programa de los institutos Confucio en todo el mundo, forma parte del sistema de propaganda de los partidos chinos; pide a los Estados miembros y a la Comisión que apoyen los cursos independientes de lengua china, sin intervención del Estado chino ni de organizaciones dependientes; cree que el Centro Nacional de China recién establecido en Suecia podría tomarse como un ejemplo destacado del modo de acrecentar en Europa las competencias independientes relativas a China;

130. Considera, además, que los institutos Confucio sirven como plataforma para el ejercicio de presiones a favor de los intereses económicos chinos, así como para las actividades del servicio de inteligencia chino y el reclutamiento de agentes y espías; recuerda que muchas universidades han decidido poner fin a su cooperación con los institutos Confucio debido a los riesgos de espionaje e injerencia chinos, como es el caso de las universidades de Dusseldorf en 2016, Bruselas (VUB y ULB) en 2019 y Hamburgo en 2020, y todas las universidades de Suecia; pide que más universidades reflexionen sobre su cooperación actual para garantizar que no afecta a su libertad académica; pide a los Estados miembros que sigan de cerca las actividades de enseñanza, investigación y de otro tipo de los institutos Confucio y que, cuando haya por pruebas claras que confirmen casos presuntos de espionaje o injerencia, adopten medidas coercitivas para salvaguardar la soberanía política y económica europea, por ejemplo, la denegación de la financiación o la retirada de las licencias de los institutos asociados;

131. Observa que la injerencia extranjera también puede llevarse a cabo mediante el ejercicio de influencia en instituciones religiosas y su instrumentalización, como en el caso de Rusia en las Iglesias ortodoxas, en particular en Serbia y Montenegro, Bosnia y Herzegovina, en particular su entidad Republika Srpska, Georgia y en cierta medida en Ucrania, entre otros medios sembrando la discordia entre poblaciones locales, desarrollando una narrativa sesgada de la historia y promoviendo una agenda contraria a la Unión, en el caso de la influencia ejercida por el Gobierno de Turquía a través de las mezquitas en Francia y Alemania, y en el caso de la influencia de Arabia Saudí a través de mezquitas salafistas en toda Europa que propugnan un Islam radical; pide a la Comisión y a los Estados miembros que garanticen una mejor coordinación en lo que atañe a la protección de las instituciones religiosas frente a la injerencia extranjera y que limiten la financiación y aumenten su transparencia; pide a los Estados miembros que sigan de cerca las actividades de las instituciones religiosas y, cuando proceda y esté justificado con pruebas, adopten medidas, como la denegación de la financiación o la retirada de las licencias de los institutos asociados;

132. pide al SEAE que presente un estudio sobre la prevalencia y la influencia de agentes estatales malintencionados en grupos de reflexión, universidades, organizaciones religiosas y medios de comunicación europeos; pide a todas las instituciones de la

Unión y a los Estados miembros que mantengan un diálogo sistemático con partes interesadas y expertos y colaboren con ellos para determinar con precisión y supervisar la influencia extranjera en los ámbitos cultural, académico y religioso; pide un mayor intercambio de contenidos entre emisoras nacionales europeas, incluidas las de los países vecinos;

133. Manifiesta su preocupación ante las noticias relativas a injerencias extranjeras en los sistemas judiciales europeos; llama la atención, en especial, sobre la ejecución por parte de órganos jurisdiccionales europeos de sentencias rusas contra oponentes del Kremlin; pide a los Estados miembros que conciencien al personal judicial y trabajen con la sociedad civil para prevenir abusos por parte de Gobiernos extranjeros de la cooperación judicial internacional y los tribunales y órganos jurisdiccionales europeos; pide al SEAE que encargue un estudio sobre la prevalencia y la influencia de la injerencia extranjera en los procedimientos judiciales europeos; señala que, sobre la base de dicho estudio, podría ser necesario proponer cambios en los requisitos de transparencia y financiación aplicables a los procedimientos judiciales;

***Disuasión, atribución y contramedidas colectivas, incluidas sanciones***

134. Considera que los regímenes de sanciones establecidos recientemente por la Unión, como las medidas restrictivas contra los ciberataques que amenazan a la Unión y sus Estados miembros[26] y el régimen de sanciones de la UE de alcance mundial en materia de derechos humanos (Ley Magnitski de la Unión)[27], adoptados el 17 de mayo de 2019 y el 7 de diciembre de 2020, respectivamente, han demostrado un valor añadido al proporcionar a la Unión herramientas de disuasión valiosas; pide a la Comisión que presente una propuesta legislativa para la adopción de un nuevo régimen de sanciones temáticas al objeto de abordar los actos de corrupción graves; recuerda que los regímenes de sanciones contra ciberataques y violaciones de los derechos humanos se han utilizado dos veces, en 2020 y 2021 respectivamente; insta a que se haga permanente el régimen de sanciones contra los ciberataques y pide a los Estados miembros que compartan todos los datos y la información que hayan allegado para contribuir a la elaboración de listas de sanciones contra los ciberataques;

135. Pide a la Unión y a sus Estados miembros que adopten nuevas medidas contra la injerencia extranjera, incluidas las campañas de desinformación a gran escala, y las amenazas híbridas, con pleno respeto de las libertades de expresión y de información, en particular mediante el establecimiento de un régimen de sanciones; considera que esto debe incluir la introducción de un marco de sanciones intersectorial y asimétrico, así como sanciones diplomáticas, prohibiciones de viaje, inmovilizaciones de activos y la retirada de los permisos de residencia de la Unión de personas extranjeras y miembros de sus familias en relación con intentos de injerencia extranjera, que deben dirigirse con la mayor precisión posible contra los responsables de la toma de decisiones y los organismos responsables de las acciones agresivas, evitando una mecánica de «ojo por ojo», de conformidad con el artículo 29 del TUE y el artículo 215 del Tratado de Funcionamiento de la Unión Europea (TFUE) (medidas restrictivas) y firmemente integrado en los pilares de la política exterior y de seguridad común (PESC) y de la

[26] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL%3A2019%3A129I%3ATOC
[27] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:L:2020:410I:TOC

PCSD de la Unión; pide a los Estados miembros que incluyan en el orden del día del Consejo de Asuntos Exteriores un punto fijo relativo a la injerencia y la desinformación procedentes del exterior y del interior; pide a la Unión que defina con claridad qué constituye un hecho internacionalmente ilícito y que establezca unos umbrales mínimos para la puesta en marcha de contramedidas como consecuencia de esa nueva definición, que deben ir acompañadas de una evaluación de impacto para aportar seguridad jurídica; señala que el Consejo debe poder tomar decisiones por mayoría, en vez de por unanimidad, sobre las sanciones relativas a injerencias extranjeras; considera que los países que intervienen en actividades exteriores de injerencia y manipulación de la información con el fin de desestabilizar la situación en la Unión deben sufragar los costes de sus decisiones y asumir las consecuencias económicas, diplomáticas y de reputación; pide a la Comisión y al vicepresidente de la Comisión y alto representante de la Unión para Asuntos Exteriores y Política de Seguridad que presenten propuestas concretas a este respecto;

136. Insiste en que, a la vez que intenta preservar los procesos democráticos, los derechos humanos y las libertades definidos en los Tratados, todo régimen de sanciones debe prestar especial atención a las repercusiones en los derechos y libertades fundamentales de las sanciones que se impongan, con el fin de preservar el respeto de la Carta de los Derechos Fundamentales, y debe ser plenamente transparente en cuanto a los motivos en que se funda la decisión de aplicar una sanciones; hace hincapié en la necesidad de una mayor claridad a escala de la Unión respecto del alcance de las sanciones y su impacto en las personas asociadas, por ejemplo, nacionales y empresas de la Unión;

137. Considera que, aunque la naturaleza de estos ataques híbridos varía, su peligro para los valores, los intereses fundamentales, la seguridad, la independencia y la integridad de la Unión y sus Estados miembros, así como para la consolidación y el apoyo a la democracia, el Estado de Derecho, los derechos humanos, los principios del Derecho internacional y las libertades fundamentales, puede ser sustancial en cuanto a la magnitud de los ataques, su naturaleza o su efecto acumulativo; acoge con satisfacción el hecho de que el Plan de Acción para la Democracia Europea prevea que la Comisión y el SEAE colaboren en el desarrollo de un conjunto de instrumentos contra las injerencias extranjeras y las operaciones de influencia, incluidas las operaciones híbridas y la atribución clara de los ataques malintencionados por parte de terceros países y partes contra la Unión;

138. Destaca que la idea de que ciertas acciones de injerencia extranjera afectan gravemente a los procesos democráticos e influyen en el ejercicio de derechos o deberes gana terreno a escala internacional; señala, en este sentido, las enmiendas adoptadas en 2018 con respecto a la Ley de modificación de la legislación australiana sobre seguridad nacional (espionaje e injerencias extranjeras), cuyo objetivo es tipificar como delito las actividades encubiertas y engañosas de agentes extranjeros que pretenden interferir en procesos políticos o gubernamentales, afectar a derechos o deberes, o apoyar las actividades de inteligencia de un Gobierno extranjero, mediante la creación de nuevos delitos como la «injerencia extranjera intencionada»;

139. Es consciente de que, de conformidad con el artículo 21, apartado 3, del TUE, la Unión debe garantizar la coherencia entre los diferentes ámbitos de su acción exterior, y entre estas y otras políticas, tal como se define en los Tratados; señala, a este respecto, que las

injerencias extranjeras, como la amenaza que representan los combatientes y los grupos terroristas extranjeros que influyen en las personas que permanecen en la Unión, también se abordó mediante la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo[28];

140. Subraya que, para reforzar su impacto, las sanciones deben imponerse colectivamente sobre la base, cuando sea posible, de la coordinación con socios de ideas afines, posiblemente con la participación de organizaciones internacionales y formalizadas en un acuerdo internacional, también con respecto a otros tipos de reacciones a los ataques; señala que los países candidatos y los potenciales países candidatos también deben adoptar estas sanciones para ajustarse a la PESC de la Unión; observa el importante trabajo realizado por la OTAN en el ámbito de las amenazas híbridas y recuerda, a este respecto, el comunicado de la reunión de la OTAN de 14 de junio de 2021, en el que se reafirma que el Consejo del Atlántico Norte adoptará, en cada caso, una decisión sobre cuándo un ciberataque conllevaría la invocación del artículo 5 del Tratado de la OTAN, y que el impacto de una acumulación de actividades cibernéticas malintencionadas significativas podría considerarse, en determinadas circunstancias, equivalente a un ataque armado[29]; hace hincapié en que la Unión y la OTAN deben adoptar un enfoque más prospectivo y estratégico en materia de amenazas híbridas, centrado en los motivos y objetivos de los adversarios, y aclarar en qué casos está la Unión mejor equipada para hacer frente a una amenaza y cuáles son las ventajas comparativas de sus respectivas capacidades; recuerda que varios Estados miembros de la Unión no son miembros de la OTAN, pero, no obstante, cooperan con ella, por ejemplo, a través de su programa de Asociación para la Paz (APP) y su Iniciativa de Interoperabilidad de la Asociación (PII), y subraya, por tanto, que ninguna cooperación entre la Unión y la OTAN debe afectar a la política de seguridad y defensa de los Estados miembros de la Unión no pertenecientes a la OTAN, incluidos los que aplican una política de neutralidad; destaca la importancia de la asistencia mutua y la solidaridad en consonancia con el artículo 42, apartado 7, del TUE y el artículo 222 del TFUE, y pide a la Unión que elabore supuestos concretos de activación de estos artículos en el caso hipotético de que se produzca un ciberataque; pide a la Unión y a todos los Estados miembros que vinculen esta cuestión a otros aspectos de sus relaciones con aquellos Estados que se encuentran tras las campañas de injerencia y desinformación, en particular Rusia y China;

***Cooperación mundial y multilateralismo***

141. Reconoce que muchos países democráticos de todo el mundo se enfrentan a operaciones de desestabilización similares llevadas a cabo por agentes estatales y no estatales extranjeros;

142. Destaca la necesidad de una cooperación mundial multilateral entre países de ideas afines en los foros internacionales pertinentes respecto a estas cuestiones de importancia crucial, en forma de una asociación basada en una interpretación común y en definiciones compartidas, con vistas a establecer normas y principios internacionales; subraya la importancia de una cooperación estrecha con los Estados Unidos y otros Estados afines para la modernización de organizaciones multilaterales; celebra, a este

[28] DO L 88 de 31.3.2017, p. 6.
[29] https://www.nato.int/cps/en/natohq/news_185000.htm

respecto, la Cumbre por la Democracia y espera que dé lugar a propuestas y acciones concretas para combatir mediante la acción colectiva las principales amenazas a las que se enfrenta la democracia en la actualidad;

143. Considera que, sobre la base de una conciencia situacional común, los socios de ideas afines deben intercambiar buenas prácticas e identificar respuestas comunes a los retos mundiales, pero también a los retos nacionales compartidos, como la imposición de sanciones colectivas y la protección de los derechos humanos y las normas democráticas; pide a la Unión que lidere el debate sobre las repercusiones jurídicas de las injerencias extranjeras, promueva unas normas de atribución y unas definiciones internacionales comunes y elabore un marco internacional para responder a las injerencias en los procesos electorales con el fin de crear un código mundial de prácticas para procesos democráticos libres y resilientes;

144. Pide a la Unión y a sus Estados miembros que consideren los formatos internacionales adecuados para hacer posible tal asociación y cooperación entre socios afines; pide a la Unión y a sus Estados miembros que inicien un proceso en el marco de las Naciones Unidas con vistas a adoptar una convención mundial para promover y defender la democracia que establezca una definición común de «injerencia extranjera»; pide a la Unión que proponga un conjunto de herramientas global para la defensa de la democracia, que se incluya en la convención y contenga acciones y sanciones conjuntas para luchar contra las injerencias extranjeras;

145. Acoge con satisfacción la declaración de la OTAN de 14 de junio de 2021, en la que se reconoce el creciente reto que plantean las amenazas cibernéticas, híbridas y otras de índole asimétrica, incluidas las campañas de desinformación, y el uso malintencionado de tecnologías emergentes y disruptivas cada vez más sofisticadas; acoge favorablemente los progresos realizados en la cooperación entre la Unión y la OTAN en el ámbito de la ciberdefensa; celebra la creación por parte de Lituania del Centro Regional de Ciberdefensa, en el que participan los Estados Unidos y los países de la Asociación Oriental; apoya una cooperación más estrecha con los países socios en materia de ciberdefensa, tanto en términos de intercambio de información como de trabajo operativo; acoge con satisfacción las conversaciones sobre el control multilateral de las exportaciones de artículos de cibervigilancia entre los Estados Unidos y la Unión en el contexto del Consejo de Comercio y Tecnología;

146. Acoge favorablemente las iniciativas ya adoptadas, en particular a escala administrativa, para compartir conocimientos sobre la situación de los ataques híbridos, incluidas las operaciones de desinformación, en tiempo real, como el sistema de alerta rápida creado por el SEAE y abierto en parte a terceros países de ideas afines, el Mecanismo de Respuesta Rápida establecido por el G7 y la División Conjunta de Inteligencia y Seguridad de la OTAN;

147. Subraya que la cooperación mundial debe basarse en valores comunes recogidos en proyectos comunes, con la participación de organizaciones internacionales como la OSCE y la UNESCO, y la creación de capacidades democráticas y una paz y una seguridad sostenibles en países que se enfrentan a amenazas similares de injerencias extranjeras; aboga por que la Unión establezca un fondo europeo de medios de comunicación democráticos para apoyar el periodismo independiente en los

(potenciales) países de la ampliación y los países de la vecindad europea, y en los países candidatos y candidatos potenciales a la adhesión; pone de relieve la necesidades prácticas, como equipos técnicos de trabajo, que expresan regularmente periodistas independientes de países vecinos;

148. Hace hincapié en la urgente necesidad de abordar la desinformación y la información errónea relativas al clima; celebra los esfuerzos de la CP26 para adoptar una definición universal de desinformación e información errónea relativas al clima y para esbozar medidas encaminadas a dar respuesta a esta cuestión; pide modelos como el Grupo Intergubernamental de Expertos sobre el Cambio Climático para elaborar un código de conducta mundial sobre la desinformación, un proceso que sentaría las bases para un Acuerdo de París sobre la Desinformación;

149. Subraya la importancia de proporcionar una perspectiva clara para los países candidatos y candidatos potenciales a la adhesión y de apoyar a los países socios y vecinos, como los de los Balcanes Occidentales y las vecindades oriental y meridional, ya que Rusia, Turquía y China tratan de utilizarlos como laboratorios para la manipulación de información y la guerra híbrida con el fin de debilitar a la Unión; considera que los Estados Unidos son un socio importante en la lucha contra las injerencias extranjeras, las campañas de desinformación y las amenazas híbridas en esas regiones; expresa su preocupación, en particular, por el papel desempeñado por Serbia y Hungría en la difusión generalizada de desinformación en los países circundantes; subraya que la Unión debe apoyar a estos países y colaborar con ellos, tal como se establece en el Reglamento IVDCI[30]; considera que sus acciones pueden consistir en promover el valor añadido y el impacto positivo de la Unión en la región, financiar proyectos destinados a garantizar la libertad de los medios de comunicación, reforzar la sociedad civil y el Estado de Derecho e intensificar la cooperación en materia de alfabetización mediática, digital e informativa, respetando al mismo tiempo la soberanía de dichos países; pide que se aumente la capacidad del SEAE a este respecto;

150. Anima a la Unión y a los Estados miembros a que intensifiquen la cooperación con Taiwán en materia de lucha contra las operaciones de injerencia y las campañas de desinformación procedentes de terceros países hostiles, incluido mediante el intercambio de mejores prácticas, enfoques conjuntos para fomentar la libertad de los medios de comunicación y el periodismo, la profundización de la cooperación en materia de ciberseguridad y ciberamenazas, la sensibilización de los ciudadanos y la mejora de la alfabetización general entre la población, con objeto de fortalecer la resiliencia de nuestros sistemas democráticos; apoya la intensificación de la cooperación entre las agencias gubernamentales, las ONG y los grupos de reflexión europeos y taiwaneses pertinentes en este ámbito;

151. Pide al Parlamento que promueva de forma activa una narrativa europea, desempeñe un papel destacado en la promoción del intercambio de información y debata sobre buenas

[30] Reglamento (UE) 2021/947 del Parlamento Europeo y del Consejo, de 9 de junio de 2021, por el que se crea el Instrumento de Vecindad, Cooperación al Desarrollo y Cooperación Internacional - Europa Global, por el que se modifica y se deroga la Decisión n.° 466/2014/UE del Parlamento Europeo y del Consejo, y se derogan el Reglamento (UE) 2017/1601 del Parlamento Europeo y del Consejo y el Reglamento (CE, Euratom) n.° 480/2009 del Consejo (DO L 209 de 14.6.2021, p. 1).

prácticas con los parlamentos asociados de todo el mundo, utilizando al efecto su amplia red de delegaciones interparlamentarias, así como las iniciativas en materia de democracia y las actividades de apoyo coordinadas por su Grupo de Apoyo a la Democracia y Coordinación Electoral; destaca la importancia de la estrecha cooperación con parlamentarios de terceros países a través de proyectos específicos para respaldar una perspectiva europea para los países candidatos y candidatos potenciales;

152. Pide al SEAE que refuerce el papel de las delegaciones de la Unión y las misiones de la PCSD de la Unión en terceros países, con el fin de consolidar su capacidad para detectar y refutar las campañas de desinformación orquestadas por agentes de Estados extranjeros y financiar proyectos educativos que refuercen los valores democráticos y los derechos fundamentales; recomienda encarecidamente la creación de una plataforma de comunicación estratégica, iniciada por el SEAE, para establecer una cooperación estructural en materia de lucha contra la desinformación y las injerencias extranjeras, que debe tener sus sede en Taipéi; pide, asimismo, a las delegaciones de la Unión que contribuyan a la lucha de la Unión contra la desinformación traduciendo a las lenguas de terceros países las decisiones de la Unión relacionadas con el país donde están ubicadas, en especial las resoluciones de urgencia del Parlamento Europeo;

153. Pide que la cuestión de la injerencia malintencionada extranjera se aborde en la próxima Brújula Estratégica de la Unión;

154. Pide la creación de un mecanismo institucional permanente en el Parlamento Europeo dedicado al seguimiento de esas recomendaciones, con el fin de abordar las injerencias extranjeras y la desinformación en la Unión de un modo sistemático más allá del mandato actual de la Comisión INGE; solicita la mejora del intercambio institucionalizado entre la Comisión, el SEAE y el Parlamento a través de este mecanismo;

°

° °

155. Encarga a su presidenta que transmita la presente Resolución al Consejo, a la Comisión, al vicepresidente de la Comisión / alto representante de la Unión para Asuntos Exteriores y Política de Seguridad y a los Gobiernos y Parlamentos de los Estados miembros.

## EXPOSICIÓN DE MOTIVOS

***Antecedentes***

El 18 de junio de 2020, el Parlamento Europeo decidió crear la Comisión Especial sobre Injerencias Extranjeras en Todos los Procesos Democráticos de la Unión Europea, en particular la Desinformación, y le encomendó el mandato de formular un enfoque a largo plazo para hacer frente a las pruebas de injerencias extranjeras en las instituciones y los procesos democráticos de la Unión y sus Estados miembros.

Un año después de la reunión constitutiva de la Comisión, celebrada el 23 de septiembre de 2020, y sobre la base de una larga serie de testimonios de diversos expertos y profesionales en la materia, la ponente puede exponer ya la realidad, el alcance y la extrema sofisticación de la infinidad de formas adoptadas por las agresivas operaciones de injerencia decididas y financiadas por agentes extranjeros contra la Unión. La ponente también puede señalar, con preocupación, la rapidez de la adaptación, la volatilidad y la aceleración de este fenómeno a través de nuevos agentes, discursos y herramientas en el plazo de un solo año.

Desde las campañas de desinformación de nueva escala relacionadas con la COVID-19 hasta los ciberataques contra entidades de autoridades públicas que incluyen las infraestructuras de salud pública, pasando por las estrategias de injerencia que integran la captación de élites y el ejercicio de presiones en el ámbito industrial, la financiación encubierta de actividades políticas, el control de centros académicos y culturales o la instrumentalización de diásporas nacionales, nuestra comisión ha venido analizando la dimensión polifacética y dinámica de este nuevo tipo de guerra cuyo propósito es socavar la cohesión social y la confianza mutua de nuestras sociedades democráticas europeas para debilitarlas.

Afortunadamente, la comisión también ha sido testigo del aumento de la sensibilización respecto a estas cuestiones cruciales, incluida la idea comúnmente compartida de que la Unión y sus Estados miembros deben dotarse con celeridad de políticas de resiliencia y herramientas de disuasión plenamente consolidadas, basadas en un enfoque que incluya a la sociedad en su conjunto, que les permitan abordar todo tipo de amenazas y ataques híbridos y, por tanto, proteger el funcionamiento sostenible de la democracia.

***Refuerzo de la resiliencia mediante la conciencia situacional, la alfabetización mediática e informativa, el pluralismo de los medios de comunicación, el periodismo independiente y la educación***

Está claro que el primer fundamento de una defensa sólida contra las injerencias extranjeras consiste en adquirir conciencia situacional. Para lograrlo, debemos pasar por dos etapas importantes: en primer lugar, debemos supervisar, catalogar y analizar los diferentes ataques de injerencia para comprender plenamente la amenaza; en segundo lugar, tenemos que asegurarnos de que todos los que deben conocer este análisis estén al tanto del mismo.

Hay muchos investigadores, organizaciones de la sociedad civil, periodistas y miembros del personal de instituciones nacionales o europeas que llevan a cabo una excelente labor en cuanto a la investigación de la amenaza, y en la Comisión INGE hemos conocido a muchos de ellos. A escala europea, la ponente valora especialmente la labor de los grupos de trabajo del StratCom del SEAE. Sin embargo, tenemos que seguir avanzado en este terreno. No podemos

aceptar que todavía no haya ningún grupo de trabajo encargado de supervisar las injerencias procedentes de China.

También debemos asegurarnos de que la información se difunda a un público más amplio. Son importantes tanto la formación dirigida a personas con funciones que pueden verse afectadas por las injerencias extranjeras como las campañas generales de sensibilización. En este contexto, la alfabetización mediática y digital es crucial para que los ciudadanos puedan interpretar y evaluar mejor la información con la que se encuentran.

Los periodistas desempeñan un papel fundamental para garantizar un clima de debate saludable. Lamentablemente, la digitalización les ha afectado económicamente, sobre todo cuando los sistemas publicitarios parecen dar ventaja a los contenidos emocionales, incluidas las opiniones y la desinformación, respecto al periodismo de calidad. Asimismo, algunos periodistas sufren a menudo campañas de acoso y amenazas organizadas cuando tratan temas delicados. Si bien es importante defender la independencia de los medios de comunicación de calidad, también lo es investigar formas de apoyar a dichos medios y a los periodistas, tanto económicamente como frente al acoso.

***Injerencias extranjeras mediante el uso de plataformas en línea***

Es evidente que el sistema actual de difusión de información a través de plataformas conduce a un clima en línea distorsionado en el que prosperan la desinformación y otros tipos de manipulación de la información. Los informes sobre filtraciones y venta de datos sensibles, los algoritmos que promueven la radicalización de contenidos y las plataformas que hacen la vista gorda ante incumplimientos inequívocos de la ley o de sus propias condiciones son tan comunes que casi nos hemos acostumbrado a su existencia y han dejado de molestarnos. Tenemos que acabar con estas tendencias.

Mantener una multitud de debates con diversos expertos ha convencido a la ponente de que el método actual de autorregulación no funciona y debe sustituirse por normas vinculantes. No podemos aceptar que agentes extranjeros puedan manipular libremente el contenido que recibimos en línea a través de las plataformas, o abusar de los sistemas de publicidad para que los anunciantes contribuyan involuntariamente a su financiación. Tampoco podemos aceptar que se permita a las plataformas no hacer nada al respecto y esto no tenga consecuencias.

Es cierto que se han producido numerosas mejoras, tanto por iniciativa de las propias plataformas como a raíz de medidas públicas como el código de buenas prácticas. Sin embargo, sin una transparencia significativa, es imposible hacerse una idea del impacto de estas acciones. También es esencial que el código de buenas prácticas, que es voluntario por naturaleza, cuente con un mecanismo de ejecución eficaz y se complemente con una legislación sólida. Además, resulta sorprendente el número de políticas contra la injerencia que se aplican únicamente a contenidos en inglés o en un número muy limitado de lenguas. No podemos aceptar una situación en la que las personas de habla letona, búlgara, griega, o incluso francesa o alemana, obtengan mucha menos protección frente la manipulación en línea que los hablantes nativos de inglés simplemente porque las plataformas dan prioridad a los contenidos en este idioma.

***Infraestructuras críticas y sectores estratégicos***

Las infraestructuras críticas son esenciales para el funcionamiento de la economía y la

sociedad. Para proteger mejor los sectores críticos, es necesario realizar esfuerzos coordinados y conjuntos en todos los sectores y a diferentes escalas: de la Unión, nacional, regional y local. La nueva Directiva de la Comisión dirigida a aumentar la resistencia de las entidades críticas constituye un importante punto de partida. No obstante, la ponente considera que la lista de infraestructuras críticas debe ampliarse para abarcar también a los medios de comunicación, así como las infraestructuras electorales, dada su respectiva importancia crucial para garantizar el funcionamiento de la Unión y sus Estados miembros, y que debe actuarse con flexibilidad en cuanto a la incorporación de nuevos sectores estratégicos en el futuro. Resulta de vital importancia que la Directiva mantenga un enfoque altamente adaptable que haga posible unas actualizaciones y modificaciones rápidas.

Además, la dependencia respecto a las inversiones extranjeras y los proveedores extranjeros de tecnología en infraestructuras críticas genera numerosas amenazas para el funcionamiento autónomo de estas infraestructuras. El impulso de la Unión hacia la autonomía estratégica y la soberanía digital es, por tanto, crucial para contrarrestar tales amenazas.

***Financiación encubierta de actividades políticas por agentes y donantes extranjeros***

Existen pruebas sólidas que demuestran que los agentes extranjeros han estado interfiriendo activamente en las elecciones democráticas y los referendos de los países europeos a través de operaciones de financiación encubiertas durante las campañas.

Estas operaciones malintencionadas ponen en riesgo la integridad de las elecciones organizadas en la Unión, ya que propician una competencia desleal entre partidos y candidatos en la asignación de recursos adicionales a algunos de los partidos (generalmente los contrarios a la Unión) no contabilizados en las declaraciones oficiales de las campañas electorales.

Según el informe de 2020 de Alliance for Securing Democracy (Alianza para asegurar la democracia) sobre fondos extranjeros encubiertos[1], Rusia, China y otros regímenes autoritarios han canalizado ya más de 300 millones USD a 33 países en la última década para interferir en procesos democráticos en más de cien ocasiones, y la mitad de estos casos atañen a acciones de Rusia en Europa.

Algunas de estas operaciones ni siquiera son ilegales, ya que se valen de las numerosas lagunas existentes entre los Estados miembros, cuyas disposiciones de las leyes electorales nacionales relativas a la financiación de actividades políticas no están armonizadas a escala de la Unión.

***Ciberseguridad y resiliencia frente a ciberataques***

La creciente digitalización de los servicios ha dado lugar a una mayor dependencia de las infraestructuras críticas respecto a los sistemas en línea, lo que aumenta su vulnerabilidad frente a los ciberataques y la exposición de los datos. El número de ciberataques ha crecido en los últimos años, y estos ataques han estado dirigidos a sectores estratégicos como la Agencia Europea de Medicamentos (EMA) y el Parlamento noruego.

[1] https://securingdemocracy.gmfus.org/covert-foreign-money/

Las capacidades fragmentadas y el escaso volumen de recursos humanos y financieros ponen de relieve la vulnerabilidad de la Unión frente a los ciberataques, que no entienden de fronteras. Por lo tanto, es imprescindible que la Unión invierta rápidamente en sus capacidades y competencias digitales estratégicas mediante la asignación de recursos adicionales, tanto humanos como financieros, para la ciberseguridad, al tiempo que garantiza un elevado nivel común de ciberseguridad en todos los Estados miembros. La Estrategia de Ciberseguridad de la UE para 2020 y la Directiva SRI 2 constituyen propuestas importantes para mejorar la ciberseguridad de la Unión, que se reforzarán en el futuro mediante la Ley de ciberresiliencia y la Política de ciberdefensa.

Además, el problema de los programas espías, como Pegasus, debe abordarse rápidamente por medio del refuerzo del marco legislativo para exigir responsabilidades a los distribuidores y usuarios de este software, y a los que hacen un uso abusivo del mismo.

***Protección de los Estados miembros, instituciones, agencias, delegaciones y misiones de la Unión***

La ciberseguridad no solo debe mejorarse en todos los Estados miembros, sino también en las instituciones de la Unión. Los recientes ciberataques contra las instituciones de la Unión han puesto de manifiesto la necesidad de una cooperación interinstitucional sólida en lo que atañe a la detección, el seguimiento y la puesta en común de información durante los ciberataques, así como la prevención de estos. Las instituciones europeas han adoptado ya medidas para reforzar su ciberseguridad, y cuentan con herramientas para coordinar y detectar ciberataques, como el CERT-EU, la ENISA y la futura unidad informática conjunta.

Sin embargo, esto no es suficiente. En primer lugar, deberían aumentarse los recursos humanos y financieros para hacer frente a los desafíos que plantea un panorama de amenazas en constante evolución. En segundo lugar, las instituciones de la Unión deben llevar a cabo una revisión exhaustiva de sus servicios y redes con el fin de atenuar los riesgos para la seguridad, y de garantizar que las instituciones no dependan de tecnologías extranjeras para su seguridad. Por último, deben garantizarse la sensibilización, formación y orientación adecuadas de todo el personal para mitigar y abordar los riesgos de seguridad cibernética y no cibernética.

***Injerencia por medio de agentes globales a través de la captación de élites, las diásporas nacionales, universidades y eventos culturales***

Otro instrumento con el que cuentan los países extranjeros dispuestos a interferir en el funcionamiento de la Unión es el de la injerencia a través de personas.

La «captación de élites» constituye, por desgracia, un fenómeno muy extendido, y su forma más conocida consiste en la contratación de antiguos políticos y funcionarios europeos de alto nivel por empresas controladas por Estados extranjeros a cambio de sus conocimientos adquiridos durante sus mandatos o su desempeño de funciones públicas. Sus conocimientos, a menudo basados en información y contactos confidenciales, se utilizan en detrimento de los intereses estratégicos de la Unión y sus Estados miembros. Estas operaciones se combinan a menudo con estrategias de ejercicio de presiones en el ámbito industrial, en las que se fusionan objetivos económicos y políticos.

Otra forma de injerencia por medio de personas es el aumento de la influencia sobre las

universidades, las escuelas y los centros culturales y religiosos y, en última instancia, el control de estas entidades por parte de agentes de Estados extranjeros, cuando se trata de temas relevantes para el país extranjero en cuestión. La forma en que los institutos Confucio, recientemente rebautizados como «centros de educación y cooperación lingüística», procuran controlar todo tipo de investigación, enseñanza o incluso exposición cultural relacionada con China en muchas universidades y museos europeos constituye un vivo ejemplo de tal práctica. Otros países también son muy activos en este campo, como es el caso de Rusia a través de las iglesias ortodoxas.

Esta forma de injerencia se vale en gran medida de los esfuerzos por controlar la diáspora nacional que reside en la Unión, lo que puede repercutir en diversos estratos de las sociedades europeas. Estos esfuerzos también tienen como objetivo silenciar a los opositores políticos que viven en el extranjero.

***Disuasión, atribución y contramedidas colectivas, incluidas sanciones***

La Unión y sus Estados miembros deben crear herramientas de disuasión creíbles. De hecho, la Unión y sus Estados miembros no disponen actualmente de ningún régimen específico de sanciones respecto a las injerencias extranjeras y las campañas de desinformación orquestadas por agentes de Estados extranjeros.

La ponente es consciente de las dificultades jurídicas que pueden plantearse al establecer este régimen de sanciones, incluida la necesidad de definir con precisión los elementos de los delitos y sus posibles efectos acumulativos de conformidad con la legislación internacional y de la Unión.

No obstante, la ponente considera que la Unión puede ser una fuente de información útil lo que han hecho otros socios a este respecto, como hizo Australia en particular al definir lo que constituye una «injerencia extranjera intencionada» y al establecer como delitos las actividades encubiertas y engañosas de agentes extranjeros.

La ponente también cree que podemos aprovechar lo que ya existe a escala de la Unión, en particular el régimen de medidas restrictivas contra los ciberataques que amenazan a la Unión y sus Estados miembros, que se utilizó en dos ocasiones el año pasado.

Por último, pero no por ello menos importante, cabe señalar la necesidad de cooperar estrechamente con nuestros socios internacionales de ideas afines en lo que atañe a cualquier régimen de sanciones, con el objetivo de imponer sanciones conjuntamente para reforzar la eficacia y el efecto disuasorio.

Las entidades extranjeras responsables de operaciones de injerencia agresivas contra las democracias no deben suponer que sus campañas de desestabilización carecerán de consecuencias.

***Cooperación mundial y multilateralismo***

La Unión dista mucho de ser la única zona democrática del mundo que se enfrenta a acciones de injerencia extranjera cada vez más agresivas. Muchos otros países, ya sean desarrollados o en desarrollo, también son objeto de tales operaciones, que son llevadas a cabo por China o Rusia y otros regímenes autoritarios y tienen siempre el mismo objetivo: socavar el

funcionamiento democrático para ganar influencia.

Debemos reunir a los socios con ideas afines para abordar estas cuestiones de manera coordinada, sobre la base de una asociación de democracias.

En primer lugar, debemos acordar definiciones comunes y tener un entendimiento común de lo que está actualmente en juego, con vistas a convenir en unas normas y unos estándares internacionales.

Las siguientes preguntas se deben formular y responder de manera precisa y colectiva: ¿qué es una injerencia extranjera agresiva?, ¿cómo se deben calificar desde un punto de vista jurídico las operaciones de desinformación y manipulación orquestadas desde un país extranjero?, ¿cómo podemos tipificar estas amenazas y ataques como delitos? y ¿qué régimen de sanciones colectivas podría aplicarse?

A continuación, debe basarse la cooperación a escala mundial en el intercambio de buenas prácticas y la gestión de proyectos concretos. El Parlamento Europeo, a través de su amplia red de foros interparlamentarios, debe desempeñar un papel fundamental en este caso, al igual que las delegaciones de la Unión en terceros países.

***Métodos de trabajo***

Independientemente de nuestra visión política sobre diferentes instrumentos legislativos y de nuestros colores en el espectro político, como miembros de la Comisión INGE, compartimos la idea de que nuestra democracia debe mantenerse firme frente a los intentos de injerencia extranjera. Por este motivo, hemos desarrollado nuestro trabajo en la comisión sobre la base de una intensa cooperación entre los distintos grupos políticos. Los coordinadores deciden conjuntamente con la presidencia a qué expertos invitar y qué estudios encargar. La ponente consultó periódicamente a los ponentes alternativos durante su labor de redacción.

Desde el punto de vista temático, podemos distinguir la fase de diagnóstico de la etapa centrada en las soluciones. Durante la primera fase, invitamos a expertos que nos podían ayudar a entender las amenazas y los métodos en todas sus variedades. Guiados por el mandato asumido, mantuvimos diversas audiencias sobre injerencias en el ámbito público y privado, e investigamos los métodos de diferentes agentes extranjeros. En la fase centrada en las soluciones, la Comisión INGE se centró en la identificación de posibles herramientas y estrategias para prevenir y contrarrestar los problemas identificados.

La Comisión INGE encargó asimismo seis estudios e invitó a los autores a presentar sus conclusiones. La situación sanitaria asociada a la pandemia de COVID-19 nos impidió organizar misiones durante los dos primeros semestres de existencia de la Comisión INGE. Sin embargo, en la fecha de redacción del presente documento, los miembros de la Comisión INGE acaban de regresar de una primera misión culminada con éxito a la Agencia de la Unión Europea para la Ciberseguridad (ENISA) en Atenas (Grecia). Están previstas otras tres misiones: a Taipéi, París y Washington.

Para seguir preparando nuestras recomendaciones, formulamos dos preguntas con solicitud de respuesta oral. En julio de 2021, preguntamos al vicepresidente / alto representante Josep Borrell, cómo pretendía remediar la falta de recursos y de mandato para los grupos de trabajo del StratCom del SEAE, además de la falta de sanciones adecuadas para los agentes

extranjeros que llevan a cabo actividades de injerencia. En octubre de 2021, preguntamos a la vicepresidenta de la Comisión, Věra Jourová, cómo pensaba garantizar que la falta de coordinación entre sectores y escalas políticos no eleve la exposición a las injerencias extranjeras, y cómo se puede mejorar la transparencia de los algoritmos y apoyar la alfabetización mediática.

Una de nuestras principales conclusiones fue la importancia de la cooperación y el intercambio de información, tanto a escala mundial como entre los distintos niveles de gobierno y diferentes sectores dentro de la Unión. Por tanto, desde el principio hemos invitado a nuestras reuniones a otras comisiones y delegaciones con competencias vinculadas a la injerencia extranjera. Los conocimientos técnicos especializados de estos órganos hermanos enriquecieron los debates que mantuvimos con los invitados y garantizaron que las conclusiones de nuestras audiencias se trasladaran a los comités ordinarios que trabajan con las correspondientes propuestas legislativas.

Un evento clave será la reunión interparlamentaria que celebraremos en noviembre de 2021. Esta reunión entre diputados de países de la Unión y de un grupo seleccionado de socios globales de ideas afines constituirá una oportunidad crucial para aprender unos de otros y debatir retos y soluciones comunes.

Para preparar el presente informe, la ponente elaboró cuatro documentos de trabajo: sobre el estado de las injerencias extranjeras en la Unión Europea, en particular la desinformación, sobre la financiación encubierta de actividades políticas por donantes extranjeros, sobre las injerencias extranjeras mediante el uso de plataformas en línea, y sobre el refuerzo de la resiliencia de la Unión frente a amenazas híbridas.

Además de todas las reuniones formales mencionadas, la ponente recabó diversos conocimientos a través de encuentros, la participación en conferencias y la lectura de un gran número de estudios y artículos periodísticos.

***Cooperación con otros órganos del Parlamento Europeo y de la Unión***

Debido a la naturaleza intersectorial de nuestro mandato, la Comisión INGE invitó a cinco comisarios y debatió diferentes aspectos de la interferencia extranjera con ellos:

- Věra Jourová, vicepresidenta de Valores y Transparencia,
- Margaritis Schinas, vicepresidente para la Promoción de Nuestro Modo de Vida Europeo,
- Josep Borrell, vicepresidente de la Comisión Europea / alto representante de la Unión para Asuntos Exteriores y Política de Seguridad,
- Thierry Breton, comisario de Mercado Interior, y
- Margrethe Vestager, vicepresidenta ejecutiva para una Europa Adaptada a la Era Digital.

Mantuvimos, asimismo, varias conversaciones con el personal de la Comisión y el Servicio Europeo de Acción Exterior, así como una reunión especial, junto con la Comisión CONT,

con el Tribunal de Cuentas Europeo sobre su Informe Especial n.º 09/2021 titulado «El impacto de la desinformación en la UE: una cuestión abordada, pero no atajada».

La Comisión INGE también ha establecido un plan de cooperación con varias comisiones del Parlamento Europeo con las que comparte algunas competencias. La Comisión INGE cuenta hasta la fecha con once comisiones y once delegaciones.

***Asesoramiento externo***

La Comisión Especial sobre Injerencias Extranjeras en Todos los Procesos Democráticos de la Unión Europea, en particular la Desinformación, ha recabado los conocimientos técnicos especializados externos sobre los siguientes temas que atañen al trabajo en curso de la Comisión:

- Desinformación - catalogación y soluciones, incluida la regulación de las plataformas
- Financiación - catalogación y soluciones
- Infraestructuras
- Buenas prácticas en el enfoque de toda la sociedad para contrarrestar las amenazas híbridas
- Impacto de las campañas de desinformación en los migrantes, el colectivo LGBTI y los grupos minoritarios
- Lecciones extraídas de los abusos cometidos por regímenes autoritarios

***Resumen de audiencias con expertos externos***

Audiencias temáticas

- **Amenazas híbridas, desinformación y polarización – visión general institucional**, 24 de septiembre de 2020
- **Injerencias electorales, financiación de partidos políticos y plataformas de redes sociales – visión general**, 2 de octubre de 2020
- **La injerencia extranjera que mina la soberanía: el ejemplo de nuestros vecinos del este**, 21 de octubre de 2020
- **Injerencias extranjeras en la esfera pública: verificación de datos, plataformas de redes sociales y su utilización para la desinformación y las injerencias extranjeras y el refuerzo de la resiliencia**, 26 de octubre de 2020 y 9 de noviembre de 2020
- **Injerencias extranjeras en el ámbito político: injerencias extranjeras durante los procesos electorales, incluidos ataques informáticos, filtraciones de datos y comunicaciones malintencionadas**, 12 de noviembre de 2020
- **Injerencias extranjeras en el ámbito político: financiación política procedente de terceros países a través de canales legales o ilegales o donaciones mediante**

**testaferros**, 2 de diciembre de 2020

- **Periodismo contra propaganda**, 11 de diciembre de 2020
- **Posibles peligros de injerencia de terceros países en un contexto geopolítico**, 25 de enero de 2021 y 1 de febrero de 2021
- **Comunicación estratégica para luchar contra las injerencias extranjeras**, 22 de febrero de 2021
- **Modos de conferir mayor transparencia a la financiación de los partidos políticos y las campañas: ¿qué normas necesita la Unión Europea?**, 23 de febrero de 2021
- **Democracia en línea: ¿cuáles son los riesgos? ¿Cómo protegernos?**, 17 de marzo de 2021
- **Injerencias extranjeras en la financiación de organizaciones contrarias al derecho a decidir en la Unión**, 25 de marzo de 2021
- **Avances tecnológicos y enfoques reguladores de la desinformación: interferencias través de la publicidad**, 13 de abril de 2021
- **Avances tecnológicos y enfoques reguladores respecto a la desinformación**, 15 de abril de 2021
- **Intercambio de puntos de vista con Mikhail Khodorkovsky, fundador del Dossier Center**, 10 de mayo de 2021
- **Audiencia con Facebook, Twitter y YouTube sobre el papel de las plataformas de redes sociales para propagar y desarrollar la desinformación y para detectarla y contrarrestarla**, 10 de mayo de 2021
- **Cómo la historia, la cultura y la educación pueden contribuir a luchar contra la desinformación**, 15 de junio de 2021
- **Desinformación y discriminación**, 12 de julio de 2021
- **El Plan de Acción para la Democracia Europea y la Ley de servicios digitales y otros instrumentos de la Unión: cómo podrían proteger las propuestas los procesos democráticos en la Unión frente a las injerencias extranjeras, y próximos pasos**, 2 de septiembre de 2021
- **Sanciones y contramedidas colectivas**, 2 de septiembre de 2021

Intercambios de puntos de vista

- **El papel de la educación, los medios de comunicación y la cultura a la hora de combatir la desinformación y las injerencias extranjeras**, 9 de septiembre de 2021,
- **Injerencias extranjeras y espionaje a políticos e instituciones europeos**, 9 de septiembre de 2021,

- **Seguridad de las instituciones de la UE: respuesta a la escalada de los ciberataques**, 9 de septiembre de 2021,

- **Perjuicios económicos de las injerencias extranjeras y la desinformación, incluido el mercado de datos**, 14 de octubre de 2021.

## POSICIÓN MINORITARIA PRESENTADA POR CLARE DALY EN NOMBRE DEL GRUPO THE LEFT

Las injerencias extranjeras suponen un grave perjuicio social y merecen especial atención, pero no son nuevas ni se producen exclusivamente en Europa. Entre los ejemplos de injerencia en los procesos democráticos en la Unión, el más relevante y sistémico es el de grandes concentraciones de capitales, tanto extranjeros como europeos, que influyen en la elaboración de la legislación y la definición de políticas.

Esto hecho apenas ha sido reconocido por la mayoría en la Comisión INGE, que prefiere mantener una narrativa engañosa sobre una Europa víctima de adversarios geopolíticos malintencionados. Se utilizó la investigación para exagerar la amenaza de la injerencia rusa y china, ignorar las causas materiales de la crisis de la legitimidad política en Europa, estigmatizar los desacuerdos con la política exterior oficial de la Unión y establecer motivos de seguridad para limitar la libertad de expresión y otros derechos fundamentales.

Así pues, el informe resultante carece de equilibrio y objetividad, ya que constituye en sí mismo desinformación. El predominio en este informe de «conocimientos especializados» procedentes de los grupos de reflexión atlantistas y de la OTAN, que presionan en favor de intereses que se benefician del conflicto, debe considerarse en sí misma una forma de injerencia extranjera. La orientación política a la que el presente informe vincula a la Unión supone un perjuicio grave y duradero para el carácter democrático de las sociedades europeas. Las generaciones futuras se arrepentirán de este documento.

## INFORMACIÓN SOBRE LA APROBACIÓN EN LA COMISIÓN COMPETENTE PARA EL FONDO

| | |
|---|---|
| **Fecha de aprobación** | 25.1.2022 |
| **Resultado de la votación final** | +: 25<br>–: 8<br>0: 1 |
| **Miembros presentes en la votación final** | Vladimír Bilčík, Andrea Bocskor, Ioan-Rareş Bogdan, Jorge Buxadé Villalba, Włodzimierz Cimoszewicz, Gwendoline Delbos-Corfield, Anna Júlia Donáth, Marco Dreosto, Nicolaus Fest, Sunčana Glavak, Raphaël Glucksmann, Markéta Gregorová, Bart Groothuis, Balázs Hidvéghi, Sandra Kalniete, Andrey Kovatchev, Jeroen Lenaers, Nathalie Loiseau, Juan Fernando López Aguilar, Morten Løkkegaard, Pierfrancesco Majorino, Lukas Mandl, Thierry Mariani, Dace Melbārde, Maite Pagazaurtundúa, Tonino Picula, Manu Pineda, Robert Roos, Andreas Schieder, Sabine Verheyen, Viola Von Cramon-Taubadel, Javier Zarzalejos |
| **Suplentes presentes en la votación final** | Clare Daly, Petra Kammerevert |

## VOTACIÓN NOMINAL

| Votación final — Proyecto en su versión modificada (votación nominal) | +<br>25/8/1 |
|---|---|

### RESULTADOS DE LA VOTACIÓN NOMINAL

**Votación nominal: Votación final**

| 25 | + |
|---|---|
| ECR | Dace Melbārde |
| PPE | Vladimír Bilčík, Ioan-Rareş Bogdan, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Jeroen Lenaers, Lukas Mandl, Sabine Verheyen, Javier Zarzalejos |
| Renew | Anna Júlia Donáth, Bart Groothuis, Nathalie Loiseau, Morten Løkkegaard, Maite Pagazaurtundúa |
| S&D | Włodzimierz Cimoszewicz, Raphaël Glucksmann, Petra Kammerevert, Juan Fernando López Aguilar, Pierfrancesco Majorino, Tonino Picula, Andreas Schieder |
| Verts/ALE | Gwendoline Delbos-Corfield, Markéta Gregorová, Viola Von Cramon-Taubadel |

| 8 | - |
|---|---|
| ECR | Jorge Buxadé Villalba, Robert Roos |
| ID | Nicolaus Fest, Thierry Mariani |
| NI | Andrea Bocskor, Balázs Hidvéghi |
| The Left | Clare Daly, Manu Pineda |

| 1 | 0 |
|---|---|
| ID | Marco Dreosto |