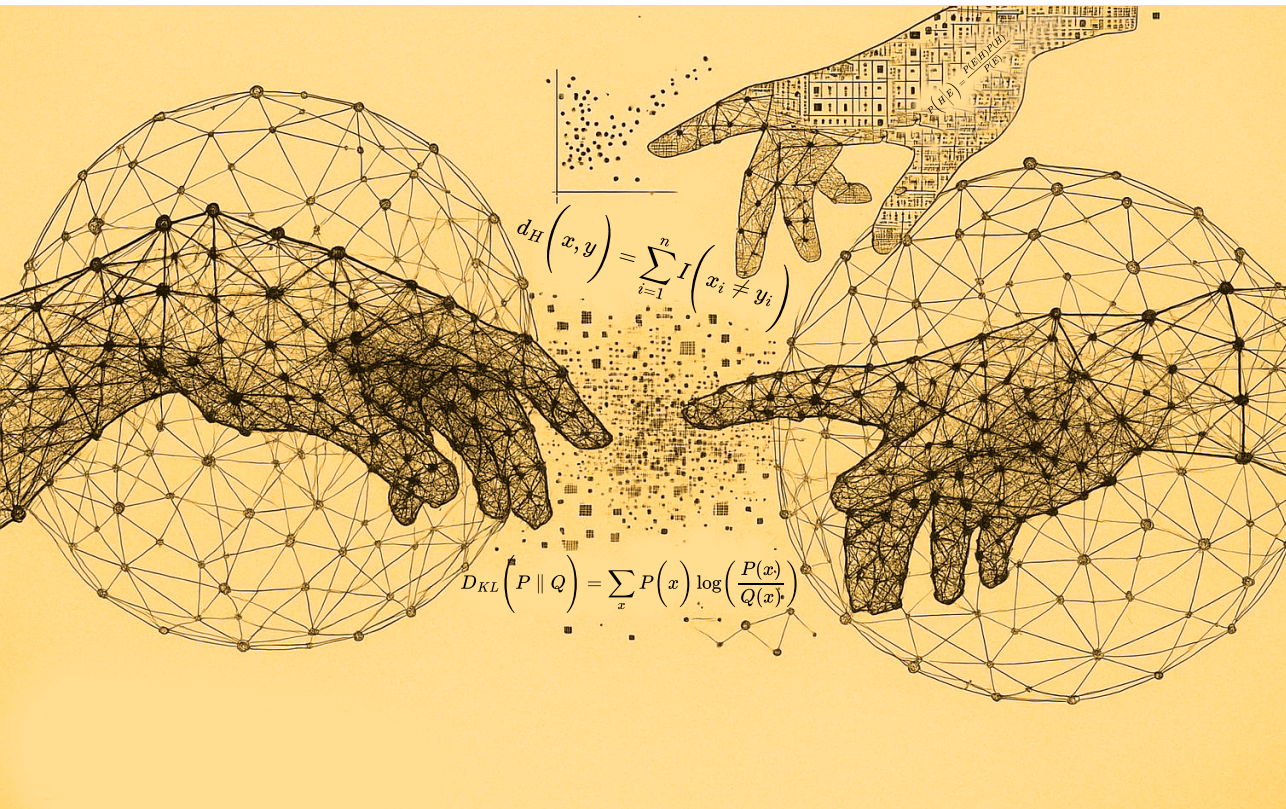
FORO CONTRA LAS CAMPAÑAS DE DESINFORMACIÓN

INICIATIVAS 2025: CONCLUSIONES Y RECOMENDACIONES DE LOS EXPERTOS

ANÁLISIS DE MECANISMOS JURÍDICOS DE DEFENSA Y RESPUESTA FRENTE A LA MANIPULACIÓN E INJERENCIA EXTRANJERA DE LA INFORMACIÓN EN ESPAÑA



ANÁLISIS DE MECANISMOS JURÍDICOS DE DEFENSA Y RESPUESTA FRENTE A LA MANIPULACIÓN E INJERENCIA EXTRANJERA DE LA INFORMACIÓN EN ESPAÑA

Todos los expertos participantes en los Grupos de Trabajo, tanto del sector público como del privado, lo son a título personal y no a título institucional. Por lo tanto, sus opiniones y recomendaciones no representan ni comprometen a las instituciones a las que pertenecen.

El resultado de los trabajos es producto de un ejercicio de reflexión colectivo, si bien, no tiene por qué representar la opinión individual de todos los participantes ni de las organizaciones o entidades públicas y privadas representadas, quienes no necesariamente comparten todas las conclusiones o propuestas.

ÍNDICE

ANÁLISIS DE MECANISMOS JURÍDICOS DE DEFENSA Y RESPUESTA FRENTE A LA MANIPULACIÓN E INJERENCIA EXTRANJERA DE LA INFORMACIÓN EN ESPAÑA

COORDINADORES

Coordinadores:

Adrián Nicolás Marchal González

Expertos del Departamento de Seguridad Nacional (DSN)

Autores y colaboradores:

Eva Campos Domínguez

Álvaro Cremades Guisado

Joaquín Delgado Martín

Carlos Galán Cordero

Francisco Pérez Bes

María Elvira Tejada de la Fuente

Expertos de la Oficina Nacional de Asesoramiento Científico (ONAC)

Expertos de la Comisaría General de Información de la PN

CONTEXTO DE LA AMENAZA DE LA FIMI

La caracterización precisa de la amenaza que representa la Manipulación e Injerencia Extranjera de la Información (FIMI, por sus siglas en inglés) constituye el marco conceptual indispensable para evaluar la adecuación y eficacia de las respuestas jurídicas disponibles.

Al objeto de evaluar dichas respuestas, se constituyó una jornada de discusión en la que participaron un conjunto de expertos de diversas áreas para que expresaran su criterio, visión y perspectiva, enfocándose en un análisis cualitativo de la amenaza de la FIMI, avanzando posibles soluciones. Este grupo de discusión contó con la presencia de:

- Adrián Nicolás Marchal González (director del Departamento de Seguridad y Defensa de la Universidad Antonio de Nebrija).
- Un representante del Departamento de Seguridad Nacional (DSN).
- María Isabel Serrano Maillo (profesora titular de Derecho Constitucional, Facultad de Ciencias de la Información de la Universidad Complutense de Madrid).
- Carlos Galán Cordero (director del Máster en Análisis de Inteligencia y Ciberinteligencia de la Universidad Antonio de Nebrija).
- María Estrella Gutiérrez David (Departamento de Derecho Constitucional, Facultad de Ciencias de la Información de la Universidad Complutense de Madrid).
- Jacobo Dopico Gómez-Aller (Catedrático de Derecho Penal en la Universidad Carlos III de Madrid).

- Francisco Pérez Bes (Adjunto a la Presidencia de la Agencia Española de Protección de Datos).

- Álvaro Cremades Guisado (director del Máster Universitario en Seguridad y Defensa de la Universidad Antonio de Nebrija).

- Joaquín Delgado Martín (Magistrado de la Sala de lo Penal de la Audiencia Nacional).

- María Elvira Tejada de la Fuente (Fiscal de Sala Coordinadora contra la Criminalidad Informática de la Fiscalía General del Estado).

- Miryam Hernández Marcos (Fiscal adscrita a la Fiscal de Sala Coordinadora de la Criminalidad informática de la Fiscalía General del Estado).

- María del Pilar Gangas Peiró (Unidad de Asesoramiento Científico del Consejo Superior de Investigaciones Científicas).

- Dos representantes de la Comisaría General de Información de la PN.

Para ilustrar y contextualizar la amenaza de las campañas de desinformación, el enfoque del Servicio Europeo de Acción Exterior (SEAE), el abanico de respuestas, los riesgos y las medidas de mitigación, se impartieron tres presentaciones a cargo tres expertos participantes, a partir de las cuales se abordaron las temáticas contenidas. Este documento pretende dinamizar dichos contenidos, compaginando los puntos de vista de los expertos y los consensos alcanzados, con marcos teóricos y conceptuales de las materias tratadas, con el propósito de poner a disposición de los lectores referencias complementarias.

A partir de las presentaciones preliminares se precisó que la amenaza primordial no radica en el contenido falso *per se*, sino en el patrón de comportamiento coordinado, intencional y manipulador desplegado por actores estatales o sus intermediarios, cuyo objetivo estratégico consiste en desestabilizar, erosionar la confianza en las instituciones democráticas o polarizar a la sociedad, entre otras.

La definición operativa adoptada por el SEAE en su primer informe sobre monitorización de amenazas FIMI establece que estas operaciones describen "un patrón de comportamiento, en su mayoría no ilegal, que amenaza o tiene el potencial de afectar negativamente a los valores, los procedimientos y los procesos políticos". Esta conceptualización resulta determinante desde una perspectiva jurídica, pues delimita el fenómeno como "una actividad de carácter manipulador, realizada de manera intencional

y coordinada por actores estatales oficiales o no estatales, incluidos sus representantes o apoderados, tanto dentro como fuera de su propio territorio". La relevancia de esta definición radica en que desplaza el análisis desde la ilicitud del contenido individual hacia la identificación de patrones sistemáticos de conducta, lo cual plantea desafíos específicos para los ordenamientos jurídicos diseñados tradicionalmente para la persecución de actos aislados.

La diferenciación conceptual entre desinformación general y operaciones FIMI es una cuestión fundamental. Mientras la desinformación tradicional suele atribuirse a un fenómeno más doméstico, de menor envergadura, aunque puede estar sostenida en el tiempo, las campañas FIMI se distinguen por diversos elementos constitutivos: coordinación sistemática, mayores recursos tecnológicos y económicos, intencionalidad estratégica y orquestado, organizado o apoyado por actores estatales.

El contenido difundido en operaciones FIMI puede no ser estrictamente ilegal considerado aisladamente, pero su dimensión lesiva deriva de la orquestación deliberada, los recursos movilizados y la finalidad desestabilizadora por parte de Estados exteriores. Esta distinción tiene derivaciones jurídicas sustanciales, pues implica que la tipicidad de las conductas no puede analizarse desde la perspectiva del contenido individual, sino que requiere una valoración holística del objetivo que se pretende con la actividad, del modus operandi y la atribución de autoría a estructuras organizadas.

La magnitud empírica del fenómeno quedó documentada mediante los datos del tercer informe del Servicio de Acción Exterior Europeo, correspondiente al período noviembre 2023 a noviembre 2024. Durante este intervalo temporal, la Unión Europea (UE) identificó 505 incidentes atribuibles a operaciones FIMI, afectando a 90 países. La infraestructura operativa de estas campañas utilizó 68,000 observables o piezas de contenido —desde memes hasta material más elaborado— distribuidos a través de 25 plataformas digitales diferentes, dirigidos contra 322 organizaciones objetivo. Estos datos cuantitativos evidencian que el fenómeno ha trascendido la fase emergente para consolidarse como una realidad estructural que amenaza persistentemente la seguridad nacional de España y de los países del entorno europeo. La dimensión transnacional del fenómeno quedó particularmente evidenciada: las acciones FIMI no entienden de fronteras geopolíticas, pues el entorno informativo digital no se circunscribe a divisiones territoriales convencionales.

El análisis de las tácticas y canales empleados reveló la existencia de un ecosistema diversificado y estratificado. El SEAE identifica cuatro categorías de actores: canales oficiales estatales (como cuentas gubernamentales o representantes de asuntos exteriores); medios de comunicación controlados por Estados (como RT y Sputnik, caracterizados por la falta de transparencia financiera, estructura organizativa y jerarquía de gestión opacas y estructuras de propiedad complejas); canales vinculados

con organismos estatales, como servicios de inteligencia; y canales directamente alineados con estas estructuras estatales. A las anteriores categorías, se destacó el potencial malicioso de una nueva categoría que podría denominarse *"usuarios de especial relevancia"*, término que debería también incluir a individuos que, con conocimiento o sin conocimiento pleno de su instrumentalización, difunden narrativas funcionales a intereses estatales extranjeros y a *influencers* cooptados mediante incentivos diversos, no necesariamente de naturaleza dineraria directa. Estos canales operarían de forma coordinada para crear una apariencia de debate social plural, cuando en realidad responden a directrices centralizadas.

Las tácticas operativas identificadas incluyen la creación sistemática de narrativas que buscan desacreditar las instituciones del Estado; el descrédito de figuras políticas mediante campañas sostenidas; socavar políticas públicas; la creación de bots y cuentas falsas para simular un debate social inexistente o amplificar el impacto, operados por redes coordinadas inauténticas; y la promoción de acciones en el mundo físico —manifestaciones, boicots— como extensión de las campañas digitales.

El caso paradigmático de Moldavia correspondiente a las elecciones de septiembre de 2025, expuesto en las presentaciones iniciales de la jornada de discusión (informe FIMI-ISAC[1] denominado "Moldova: Country Election Risk Assessment"), ilustró la sofisticación táctica: se desplegaron narrativas antieuropeas, antioccidentales, anti-Estado y prorrusas; se utilizó la aplicación Taito[2] —accesible principalmente vía Telegram— para, en principio, remunerar económicamente a ciudadanos moldavos que realizaran propaganda prorrusa y boicotearan colegios electorales; se activaron cuentas coordinadas para generar una percepción artificial de rechazo social a los resultados electorales; y finalmente se convocaron manifestaciones físicas para cuestionar la legitimidad del proceso democrático. Este ejemplo demuestra la progresión estratégica: del espacio digital al territorio físico, de la percepción a la acción.

En el contexto español, se mostraron varios casos concretos que evidencian la materialización de estas amenazas. Por ejemplo, se identificó, en las últimas elecciones generales, la suplantación de las páginas web oficiales de la Comunidad de Madrid y del Ministerio del Interior durante las últimas elecciones generales, difundiendo un mensaje falso sobre supuestos atentados de ETA en puntos de votación, dirigido inicialmente a la diáspora rusa en España como vector de amplificación.

---

[1] https://fimi-isac.org/wp-content/uploads/2025/09/Country-Report-Moldova-Risk-Assessment.pdf

[2] Aplicación que permite jugar a distancia a máquinas recreativas desde una aplicación en el teléfono móvil e ir recibiendo premios. Ofrece una amplia variedad de juegos, desde clásicos de arcade hasta realidad virtual. Puede utilizar los datos GPS para ofrecer información personalizada.

Los principales riesgos para la seguridad nacional fueron categorizados en múltiples dimensiones. En primer término, la interferencia en procesos electorales mediante la manipulación del debate público y la generación de percepciones falsas sobre legitimidad democrática. En segundo lugar, la erosión de la cohesión social a través de la amplificación de fracturas preexistentes y la creación artificial de polarización mediante el fomento de discursos extremos. Se enfatizó en los impactos en la salud pública, documentados durante la pandemia de la COVID-19, cuando la desinformación sobre vacunas condicionó decisiones sanitarias de la población. Se identificó además el potencial impacto en el deterioro de relaciones internacionales, cuando actores estatales extranjeros tratan de manipular la percepción española sobre conflictos geopolíticos o de generar incidentes diplomáticos mediante suplantación de posicionamientos oficiales. Finalmente, se constató el riesgo de perturbación del orden público, ejemplificado en el caso hipotético —pero técnicamente factible— de difusión masiva de noticias falsas sobre desabastecimiento que provocaran concentraciones multitudinarias con riesgos sanitarios o de seguridad.

En definitiva, las campañas FIMI constituyen una de las principales amenazas actuales para la seguridad nacional, precisamente por su capacidad para operar en umbrales subliminales de ilicitud, aprovechando los marcos de protección de derechos y libertades fundamentales propios de sociedades democráticas. La sofisticación de estas operaciones radica en su habilidad para instrumentalizar los valores democráticos —libertad de expresión, pluralismo informativo— como vectores de su propia desestabilización, donde las conductas individuales no alcanzan el umbral de tipicidad penal, pero su agregación coordinada produce efectos lesivos de magnitud estratégica. Esta caracterización del fenómeno condicionó decisivamente el debate posterior sobre las respuestas jurídicas disponibles y su adecuación a una amenaza de naturaleza híbrida, que opera simultáneamente en el ámbito informacional, cognitivo y, ocasionalmente, físico.

MECANISMOS DE DISUASIÓN Y MITIGACIÓN

La presentación de un informe sobre desinformación, basado en la revisión de la literatura científica y en entrevistas con expertos, identificó consensos en torno a riesgos, amenazas y medidas de respuesta —presentados al grupo de trabajo— y planteó, además, interrogantes sobre la capacidad jurídica para regular determinados aspectos del fenómeno en el ámbito digital. No obstante, el análisis transversal evidenció que un problema complejo como la FIMI requiere medidas de carácter transversal, predominantemente preventivas, orientadas a la construcción de resiliencia social y su compatibilidad *prima facie* con los marcos de protección de derechos fundamentales. Ahora bien, la convergencia en torno a estos instrumentos no supone la existencia de evidencia empírica concluyente sobre su efectividad, sino más bien el reconocimiento de su idoneidad conceptual y su reiterada consideración como útiles en la literatura especializada y en las entrevistas realizadas a expertos internacionales.

Como **primer eje** de generación de debate, la alfabetización mediática y digital emergió como la medida con mayor grado de consenso en la literatura y expertos consultados, fundamentada en la premisa de que la construcción de capacidades críticas en la ciudadanía constituye el vector más sostenible de protección frente a operaciones de manipulación informativa. Los expertos presentaron dos modelos de referencia internacional con características diferenciadas. El modelo finlandés se estructura como un currículo transversal implementado desde las etapas más tempranas de la educación primaria, diseñado específicamente para desarrollar capacidades de identificación de amenazas informacionales, con particular énfasis en operaciones atribuibles a actores estatales rusos dado el contexto geopolítico de Finlandia. Este modelo se caracteriza por su integración sistémica en el sistema educativo, no como asignatura aislada sino como competencia transversal que impregna distintas áreas curriculares.

En Estonia, por su parte, se ha fortalecido un ecosistema de verificadores de datos independientes apoyados institucionalmente por estructuras gubernamentales. Estos verificadores no solo desempeñan funciones de *fact-checking* reactivo, sino que desarrollan programas divulgativos regulares, incluyendo espacios en televisión pública que facilitan a la ciudadanía cuáles son las técnicas de manipulación informativa y operaciones de actores diversos. Estos verificadores cuentan con infraestructura y reconocimiento que les permite actuar como contrapeso informacional efectivo.

La implementación de programas de alfabetización mediática plantea, no obstante, desafíos de temporalidad evidente: se trata de inversiones cuyos efectos se materializan en plazos

generacionales, lo cual contrasta con la urgencia de las amenazas actuales. Esta limitación temporal fue expresamente reconocida por los participantes, quienes enfatizaron que la alfabetización mediática constituye una condición necesaria pero insuficiente para la protección inmediata frente a campañas FIMI en curso. La necesidad de complementar estas estrategias educativas con mecanismos de respuesta más inmediatos articuló el consenso hacia otras líneas de actuación.

El **segundo eje** se estructuró en torno a la gestión operativa de la amenaza en tres fases: monitorear, prevenir y responder.

Marco conceptual ampliatorio:

Esta secuencia refleja una concepción de la lucha contra la desinformación como proceso continuo que requiere capacidades de prevención, detección (entendida como la observación permanente del entorno informativo e identificación temprana de campañas emergentes) y activación de respuestas proporcionadas. Se enfatizo la relevancia crítica de la fase de monitorización, pues la alerta temprana constituye el presupuesto indispensable para cualquier respuesta eficaz. La constatación empírica de que las campañas FIMI despliegan sus efectos con extrema rapidez — donde la amplificación viene facilitada por los algoritmos de las plataformas y por las redes de cuentas coordinadas—, implica que la detección tardía reduce drásticamente la efectividad de cualquier contramedida.

La implementación operativa de este modelo en tres fases requiere, la definición de protocolos específicos, el establecimiento de métricas objetivas de evaluación y la dotación de capacidades técnicas para el análisis de grandes volúmenes de datos en tiempo real. La necesidad de articular mecanismos de coordinación fluida entre las entidades con capacidades de monitorización — incluyendo servicios de inteligencia, fuerzas y cuerpos de seguridad, organismos reguladores y academia— fue identificada como requisito estructural para la operatividad del modelo, más allá de la capacidad individual de los distintos organismos y órganos nacionales.

El fortalecimiento de los medios de comunicación tradicionales y medios y redes comunitarias locales constituyeron el **tercer y cuarto elementos** derivados del consenso de la literatura científica y los expertos. Los medios tradicionales, sujetos a marcos de responsabilidad consolidados y a códigos deontológicos profesionales, pueden desempeñar

funciones de vector de resiliencia y de provisión de conocimiento situacional sobre la amenaza. Esta valoración parte del reconocimiento de que, pese a las transformaciones del ecosistema mediático y la migración de audiencias hacia plataformas digitales —particularmente acusada en población juvenil—, los medios tradicionales conservan capacidades de verificación, recursos periodísticos y legitimidad institucional que las plataformas digitales no siempre poseen.

Las redes comunitarias locales fueron identificadas como eslabones particularmente relevantes, pues combinan proximidad territorial con credibilidad derivada del conocimiento situacional. Diversos expertos señalaron que los mensajes de alfabetización mediática y las advertencias sobre campañas de desinformación resultan más efectivos cuando provienen de líderes naturales con arraigo local que cuando se emiten desde estructuras centralizadas que pueden ser percibidas como distantes.[3]

La adopción de un enfoque de regulación ágil, inspirado en las recomendaciones de la OCDE, concitó igualmente consenso entre los participantes. Este modelo regulatorio se caracteriza por su naturaleza iterativa: implementación de ajustes normativos graduales, evaluación empírica de su impacto mediante métricas definidas ex ante, y refinamiento sucesivo basado en evidencia. El informe presentado por el CSIC, a través de la consulta a expertos externos, enfatizaron que la velocidad de transformación del ecosistema digital —con la emergencia constante de nuevas plataformas, funcionalidades y vectores de manipulación— torna inviable el modelo tradicional de regulación, caracterizado por procesos legislativos prolongados que producen marcos normativos rígidos. La regulación ágil implica la atribución de competencias normativas de desarrollo a autoridades administrativas especializadas, con capacidad para adaptar el marco regulatorio mediante procedimientos expeditos, sujetos a validación legislativa posterior y a evaluación continua de impacto.

Este enfoque regulatorio presenta, no obstante, tensiones con principios constitucionales de reserva de ley y seguridad jurídica, particularmente cuando las materias reguladas afectan a derechos fundamentales, especialmente a las libertades informativas (libertad de expresión y derecho a la información). La implementación de regulación ágil en el ámbito de la desinformación requiere el diseño cuidadoso de marcos habilitantes que definan con precisión taxativa los límites de la potestad reglamentaria, garanticen procesos de consulta pública y establezcan mecanismos de control jurisdiccional efectivo. La referencia al modelo OCDE no debe interpretarse, por tanto, como una

[3] Esta perspectiva conecta con literatura sobre difusión de innovaciones que enfatiza el rol de conectores locales en la adopción de comportamientos. La operativización de esta línea estratégica plantea, sin embargo, interrogantes sobre cómo identificar, formar y apoyar a estos vectores locales sin comprometer su autonomía o generar percepciones de instrumentalización.

transferencia acrítica de metodologías diseñadas para sectores con menor incidencia en derechos fundamentales, sino como una orientación metodológica que requiere adaptación sustancial al ordenamiento constitucional español.

El **quinto eje** se articuló en torno a la conveniencia de exigir mayor responsabilidad a las plataformas digitales. Se identificó que el modelo de negocio de estas plataformas —basado en la "economía de la atención"— genera incentivos estructurales para la viralización de contenido polémico y divisivo, pues estos contenidos maximizan el *engagement* y, consecuentemente, los ingresos publicitarios. Esta alineación puede suponer un problema sistémico cardinal: ¿las plataformas lucran con la polarización? Las medidas en este ámbito se mencionaron:

- Mayor responsabilidad legal de las plataformas digitales.

- La exigencia de mayor transparencia algorítmica de redes sociales, proporcionando acceso para auditorías sobre funcionamiento de algoritmos de recomendación y moderación.

- La desmonetización activa, eliminando los incentivos económicos para la producción de desinformación.

- Abordar el efecto amplificador esperado de la Inteligencia Artificial (IA) sobre la desinformación, regulando aspectos como las *deepfakes*.

- El apoyo institucional a verificadores independientes mediante acceso preferente a datos y herramientas de *fact-checking* integradas en las plataformas.

- La mejora sustancial de los códigos de autorregulación, transformándolos de instrumentos voluntarios con escaso *enforcement*, hacia códigos de conducta con consecuencias tangibles por incumplimiento.

La aplicación rigurosa del Reglamento europeo de Servicios Digitales —Digital Services Act (DSA)— fue identificada como uno de los instrumentos normativo disponible para operativizar estas exigencias. Particularmente relevante resulta el artículo 40 del DSA, que habilita el acceso de investigadores -autorizados para ello por el coordinador de servicios digitales- a datos no públicos de plataformas, generando así la infraestructura empírica indispensable para la investigación sobre campañas FIMI. Los expertos señalaron, sin embargo, que la efectividad del DSA depende actualmente de la adecuación de la normativa interna a las exigencias que plantea la aplicación en España del Reglamento, todavía no completada, que dote de eficacia disuasoria a las obligaciones establecidas en el mismo.

Una línea específica de consenso, particularmente relevante desde la perspectiva jurídica, se refirió al combate de *bots* maliciosos. Los participantes subrayaron que los *bots* —entendidos como cuentas automatizadas o coordinadas que simulan comportamiento humano— no tienen personalidad jurídica y, por tanto, no son titulares de derechos fundamentales, lo cual elimina las objeciones constitucionales que complican otras intervenciones sobre dichas cuentas. La detección y eliminación de comportamiento coordinado inauténtico debe constituir, según el consenso alcanzado, una obligación exigible a las plataformas. Esta línea de actuación se fundamenta en que la generación artificial de apariencias de debate social —mediante miles de cuentas falsas que amplifican determinadas narrativas— constituye una forma de manipulación del espacio público que no merece protección bajo el paraguas de la libertad de expresión. La viabilidad técnica de esta medida quedó, no obstante, condicionada a la cooperación efectiva de las plataformas, pues solo ellas disponen completamente de la información técnica necesaria para identificar patrones de comportamiento inauténtico a escala. No obstante, se debe explorar las posibilidades de la IA como herramienta para mejorar la monitorización de comportamientos manipulativos y de las tácticas, técnicas y procedimientos (TTP).

RESPUESTA JURÍDICA: ANÁLISIS DE LA VÍA PENAL

Opciones y limitaciones del Derecho Penal

El análisis de las posibilidades de respuesta penal frente a operaciones FIMI generó un consenso técnico transversal entre los juristas participantes: el Derecho Penal constituye una herramienta difícil de aplicar y estructuralmente poco ágil para combatir la mayoría de las campañas de manipulación e injerencia informativa extranjera. Este consenso no deriva de una valoración abstracta sobre la conveniencia de la criminalización, sino de la constatación empírica de obstáculos dogmáticos, procesales y constitucionales que tornan extremadamente compleja la subsunción de estas conductas en los tipos penales existentes y que plantean serias dudas sobre la viabilidad constitucional de eventuales reformas legislativas orientadas a tipificar específicamente la desinformación, por el peligro de que las libertades informativas pudieran verse conculcadas.

Igualmente, se sugirió la conveniencia de considerar la identificación de nuevos casos penales que se ajusten a la realidad de las operaciones FIMI, si se constatan nuevos bienes jurídicos necesitados de especial protección. Específicamente, alguno de los participantes se refirió a los delitos que comprometen la paz o la independencia el Estado o los relativos a la Defensa Nacional.

Uno de los expertos del ámbito jurídico expresó de forma categórica que ofrecer una respuesta de entrada en la desinformación vía penal es extremadamente difícil, pero no imposible. Esta caracterización sintetiza la postura dominante en el debate: la vía penal no está absolutamente clausurada, pero su operatividad queda circunscrita a supuestos muy específicos donde concurren elementos adicionales que haga posible la adecuada concreción de las conductas que se considera conveniente tipificar por afectar a bienes jurídicos necesitados de protección penal. La dificultad no radica en deficiencias técnicas de los tipos penales existentes dentro de su ámbito de protección originario, sino en que las operaciones FIMI se caracterizan precisamente por operar en umbrales que no alcanzan la tipicidad penal cuando se analizan las conductas de forma atomizada.

Otro de los expertos jurídicos participantes reforzó este diagnóstico desde la perspectiva judicial: "el derecho penal siempre llega tarde, porque el daño ya se ha producido". Esta constatación temporal resulta cardinal: la efectividad de las campañas FIMI radica en su capacidad de generar percepciones, moldear narrativas y erosionar confianzas en períodos temporales muy breves, frecuentemente amplificadas por dinámicas de viralización algorítmica. Cuando el sistema de justicia penal —con sus garantías procesales, sus

plazos de investigación, sus requisitos probatorios— alcanza a pronunciarse, el daño al bien jurídico protegido ya se ha consumado irreversiblemente. El proceso penal puede eventualmente generar efectos de prevención general negativa mediante la sanción ejemplarizante, pero resulta estructuralmente inadecuado para la prevención inmediata o la interrupción temprana de campañas en desarrollo.

Esta limitación temporal se ve agravada por el carácter de última ratio del Derecho Penal en el ordenamiento jurídico español. Los participantes enfatizaron que la intervención punitiva del Estado únicamente resulta legítima cuando otros mecanismos de protección de bienes jurídicos han resultado insuficientes y cuando la gravedad de la lesión justifica la imposición de las sanciones más severas que el ordenamiento contempla. En el ámbito de la desinformación, donde frecuentemente se contraponen bienes jurídicos protegidos con jerarquía semejante —libertad de expresión e información, orden público o seguridad nacional— el principio de proporcionalidad exige una fundamentación particularmente robusta de la necesidad de criminalización. Los expertos constataron que esta exigencia de subsidiariedad obliga a explorar exhaustivamente las vías administrativas y civiles[4] antes de recurrir al reproche penal.

El consenso sobre las limitaciones de la vía penal no implica, sin embargo, su irrelevancia absoluta. Algunos participantes identificaron dos funciones específicas donde la tipificación penal conserva utilidad estratégica. En primer término, la existencia de tipos penales genera un efecto de prevención general que puede disuadir conductas en determinados contextos, particularmente cuando los potenciales infractores son personas físicas operando en territorio nacional o sujetas a la jurisdicción española. La tipificación penal establece un mensaje normativo sobre la gravedad de ciertas conductas que trasciende la mera aplicación judicial concreta. En segundo lugar, la apertura de procedimientos penales habilita la adopción de medidas cautelares de intervención inmediata estimadas por la autoridad judicial, incluida la retirada de contenidos, la posibilidad de interrupción de determinados servicios o del bloqueo de unos y otros cuando radican en el extranjero, que pueden resultar operativamente más relevantes que la eventual imposición de pena. El tipo penal puede operar, así, como fundamento habilitante de intervenciones procesales urgentes, independientemente de que el procedimiento no culmine en condena en casos como, por ejemplo, cuando los posibles autores no puedan ser identificados o no puedan ser puestos a disposición de los tribunales.

---

[4] Algún experto participante hizo mención a la Directiva (UE) 2022/2555, conocida como NIS 2, que regula, entre otros, la responsabilidad personal de los órganos de gobierno si la empresa incumple las instrucciones y requerimientos de los CSIRT competentes. Solo en el caso de llegar a considerar que una acción FIMI forma parte de un problema de ciberseguridad, podría ser una vía eficaz para explorar respuestas contra la difusión.

Los expertos en derecho constitucional presentes enfatizaron que cualquier expansión del Derecho Penal en este ámbito debe realizarse con extrema cautela, atendiendo al núcleo esencial de la libertad de expresión y al riesgo de generar efectos inhibidores sobre el debate público legítimo. La jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos establece que las restricciones a la libertad de expresión únicamente resultan proporcionadas cuando persiguen fines legítimos mediante medios necesarios y cuando la lesión al derecho es la mínima imprescindible para la protección del bien jurídico contrapuesto. En sociedades democráticas, la libertad de expresión goza de una posición preferente que obliga a interpretar restrictivamente cualquier tipo penal que pueda incidir sobre ella. Esta doctrina constitucional fue caracterizada por los participantes como la restricción dogmática fundamental que condiciona las posibilidades de criminalización de la desinformación, incluido el fenómeno de FIMI.

El necesario respecto a la libertad de expresión

La tensión estructural entre la persecución penal de campañas desinformativas y la protección constitucional de la libertad de expresión emergió como el obstáculo dogmático cardinal identificado por los participantes. Esta tensión no constituye una dificultad técnica superable mediante refinamientos legislativos, sino a un conflicto que frecuentemente se plantea en este ámbito entre bienes jurídicos de rango constitucional cuya armonización requiere ponderaciones caso por caso que difícilmente pueden predeterminarse mediante reglas generales.

Se ilustró esta problemática mediante la referencia a los delitos de odio, ámbito donde la Fiscalía ha desarrollado especialización significativa. El inconveniente de poder formular o de formular una acusación en un delito de odio radica en la delimitación de hasta dónde llega la libertad de expresión o de información y a partir de qué momento constituye una conducta prohibida. La delimitación en el caso concreto presenta elevada complejidad y requiere una valoración casuística con escrutinio estricto de los derechos en conflicto. Esta dificultad de delimitación, reconocida en un ámbito donde existe tipificación expresa y jurisprudencia consolidada, se incrementa cuando se trata de conductas donde el contenido expresivo constituye el elemento nuclear de la acción típica. La diferenciación entre opinión legítima —aunque ofensiva, irritante o socialmente perjudicial— y manifestación punible requiere valoraciones sutiles que frecuentemente solo pueden realizarse *ex post* mediante análisis contextual exhaustivo.

Los expertos en derecho constitucional subrayaron que la doctrina del Tribunal Constitucional sobre límites a la libertad de expresión establece un examen tripartito: la restricción debe perseguir un fin constitucionalmente legítimo, debe ser necesaria en una sociedad democrática, y debe resultar proporcionada en sentido estricto. En opinión

de alguno de los exertos, el primer requisito —legitimidad del fin— resulta generalmente satisfecho cuando se invoca la protección de la seguridad nacional, el orden público o el funcionamiento del sistema democrático. El segundo requisito —necesidad— exige demostrar que no existen medios alternativos menos lesivos para la libertad de expresión que puedan proteger equivalentemente el bien jurídico. Esta prueba de necesidad resulta particularmente exigente en el contexto de campañas FIMI, pues obliga a fundamentar por qué las vías administrativas, civiles o meramente políticas resultan insuficientes. El tercer requisito —proporcionalidad estricta— demanda que el sacrificio impuesto a la libertad de expresión no resulte desmesurado en relación con la importancia del objetivo perseguido y la efectividad de la medida para alcanzarlo.

La aplicación de este examen tridimensional a supuestos de desinformación genera tensiones argumentativas significativas. La mera falsedad de una manifestación, o incluso su carácter deliberadamente engañoso, no constituye, *per se*, fundamento suficiente para su criminalización si no concurren elementos adicionales que cualifiquen la gravedad de la conducta y el riesgo o daño generado para bienes jurídicos necesitados de protección penal. Múltiples participantes reiteraron que en sociedades democráticas existe un derecho a expresar opiniones sesgadas o polémicas que pueden resultar socialmente perjudiciales o despreciables. La protección constitucional no se circunscribe solo a manifestaciones políticamente correctas o razonables, sino que se extiende a expresiones que pueden resultar profundamente perturbadoras para sectores mayoritarios de la población.

Esta protección amplísima del contenido expresivo plantea interrogantes sobre los criterios que permitirían distinguir la libertad de expresión constitucionalmente protegida de otros supuestos. Algunos participantes identificaron que la jurisprudencia constitucional ha desarrollado algunos criterios objetivables: cuando la expresión constituye una incitación directa e inminente a la comisión de actos violentos o ilegales, cuando supone una intromisión ilegítima en el honor de terceros mediante imputaciones fácticas demostrablemente falsas realizadas con conocimiento de su falsedad o temerario desprecio hacia la verdad, o cuando constituye un discurso de odio que promueve la discriminación, hostilidad o violencia contra grupos especialmente vulnerables. Estos criterios, sin embargo, resultan de compleja aplicación a campañas FIMI donde frecuentemente no existe incitación explícita a la violencia, no se difaman personas concretas mediante imputaciones fácticas falsas, y no se articula un discurso de odio contra colectivos protegidos.

La jurisprudencia del TJUE y del TEDH resulta especialmente pertinente para fijar los estándares con los que deben examinarse las normativas nacionales que limitan o restringen las libertades de expresión e información —o que establecen disposiciones sancionadoras que las afectan— por razones de defensa y seguridad nacional, así

como para la prevención, investigación y enjuiciamiento de delitos graves. Un campo paradigmático es la legislación sobre conservación y acceso a datos de tráfico, que ha generado numerosos pronunciamientos del TJUE (y algunos del TEDH) respecto de normas de los Estados miembros. Aunque estas decisiones aplican el triple juicio clásico de proporcionalidad aludido anteriormente, añaden cautelas específicas al escrutar legislaciones concretas y, además, gradúan el nivel de injerencia conforme a la gravedad y al tipo de bien jurídico lesionado.

En consecuencia, deviene necesario proyectar dicha doctrina como criterio de interpretación en el diseño normativo, máxime cuando incida limitativamente sobre las libertades de expresión e información. Una regulación concebida para combatir la FIMI, cuando está deficientemente calibrada, puede acabar produciendo efectos restrictivos no justificados sobre la publicación de informaciones y opiniones legítimas, amparadas por el art. 10 CEDH y por el art. 20 CE. En la misma línea, el TEDH ha establecido criterios sobre la proporcionalidad de las sanciones administrativas que pueden imponerse en este ámbito, criterios que deberían considerarse cuidadosamente al diseñar instrumentos propios del derecho administrativo sancionador.

Asimismo, los debates evidenciaron divergencias interpretativas significativas entre los participantes sobre si determinadas conductas vinculadas a campañas FIMI —particularmente aquellas protagonizadas por *influencers* que difunden sistemáticamente narrativas favorables a intereses de potencias extranjeras— pueden ser objeto de reproche penal o si, por el contrario, constituyen ejercicio legítimo de libertades comunicativas. Algún participante sostuvo que cuando existe financiación encubierta por actores estatales extranjeros, coordinación sistemática y finalidad desestabilizadora, además de otros elementos como la cooptación, las relaciones continuadas, de cualquier clase, y el perjuicio al Estado, concurren elementos que trascienden la mera expresión de opiniones y que podrían justificar la valoración punitiva. Otros participantes argumentaron que tales acciones, incluso por actores extranjeros hostiles, no transmuta automáticamente una opinión legítima en conducta punible, y que la criminalización de opiniones basándose en la identidad del financiador generaría precedentes sumamente peligrosos para la libertad de expresión.

Adicionalmente, diversas intervenciones señalaron la obligatoriedad de que los *influencers* informen sobre cuáles contenidos que propagan son de carácter comercial, de acuerdo con la normativa de competencia desleal (art. 26.1 de la Ley 3/1991, de 10 de enero), con la obligación (arts. 20 y 21) de información y transparencia de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, y la normativa de protección del consumidor (arts. 8, 19, 47 y 49 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios). Esta divergencia interpretativa ilustra la complejidad de las ponderaciones constitucionales implicadas.

Propuestas de reforma penal

Pese al consenso sobre las limitaciones estructurales de la vía penal, se identificaron ámbitos específicos donde reformas legislativas precisas podrían ampliar las capacidades de respuesta sin comprometer desproporcionadamente la libertad de expresión. Estas propuestas se caracterizan por su precisión estratégica: no pretenden crear un tipo penal general de desinformación, sino afinar tipos existentes o colmar lagunas puntuales donde existe consenso sobre la necesidad de protección penal, como puede ser el caso de la suplantación de identidad.

Tipificación de la suplantación de identidad

La creación de un tipo penal autónomo de "usurpación de identidad digital" se concibió como una reforma esencial. Esta necesidad se fundamenta en varios elementos: la usurpación de identidad constituye un instrumento cardinal en campañas FIMI, la conducta no constituye ejercicio de libertad de expresión merecedora de protección constitucional, existe ya un bien jurídico reconocido —la identidad— susceptible de protección penal, y la tipificación no generaría efectos inhibidores sobre debate público legítimo.

El Código Penal español vigente únicamente tipifica la usurpación del estado civil (artículo 401), que implica atribuirse o ejercer los derechos, facultades y acciones de otra persona, exigiéndose cierta continuidad temporal en la suplantación, y que resulta inaplicable a la suplantación de identidad en entornos digitales. Los debates documentaron múltiples casos donde la suplantación opera como vector de operaciones FIMI: creación de perfiles falsos que suplantan a medios de comunicación legítimos para difundir noticias falsas con apariencia de credibilidad institucional, suplantación de páginas web oficiales de instituciones públicas —como ocurrió con la Comunidad de Madrid y el Ministerio del Interior—, creación de cuentas que se hacen pasar por personas públicas para difundir declaraciones falsas atribuidas a estas figuras, suplantación de personas físicas ordinarias para perpetrar fraudes o generar descrédito. La suplantación de identidad digital está facilitando fraudes, ataques contra menores, y daños reputacionales contra personas cuyos datos personales son apropiados para crear perfiles falsos, hechos cuya incidencia se constata actualmente con mayor gravedad e intensidad como consecuencia de las posibilidades que ofrecen los sistemas basados en IA.

La propuesta consensuada establece que debe tipificarse como delito autónomo la suplantación de identidad, tanto de personas físicas como jurídicas, precisando "siempre que sea en condiciones tales que pueda conducir a error sobre la identidad".

Esta delimitación pretende excluir del tipo conductas de parodia, sátira o ficción donde resulta evidente para el receptor razonable que no existe identidad real, concentrando la protección en supuestos donde la suplantación puede efectivamente engañar a terceros, sin perjuicio de lo que regule la normativa específica de protección de datos.

Asimismo, se enfatizó que la tipificación debe configurarse como delito autónomo, no requiriendo que la usurpación sea medio para la comisión de otro delito. Esta estructura típica resulta esencial, pues permite la intervención penal y la adopción de medidas cautelares —incluida la retirada de perfiles falsos— tan pronto se acredita la usurpación, sin necesidad de aguardar a que se consume un delito ulterior. El bien jurídico protegido es la identidad misma, no los eventuales perjuicios derivados de su usurpación.

La extensión de la protección a personas jurídicas resulta particularmente relevante para combatir campañas FIMI que operan mediante la creación de entidades mediáticas falsas que se presentan como medios de comunicación legítimos o mediante la suplantación de instituciones públicas.

Reforma de delitos existentes

Se identificaron varios tipos penales existentes cuya redacción actual, concebida para realidades pretéritas, podría ser objeto de adaptación para ampliar su ámbito de aplicación a conductas vinculadas con campañas FIMI, sin que ello implique una expansión desproporcionada del *ius puniendi*.

El artículo 561 del Código Penal, que tipifica la falsa alarma de emergencias (delitos contra el orden público), fue señalado como susceptible de reforma.

La propuesta de reforma planteada por alguno de los expertos juristas se orienta en adaptar este precepto para incluir la difusión de noticias falsas que generen un riesgo grave para la seguridad colectiva, incluso sin necesidad de que se produzca la movilización de servicios de emergencia. La reforma propuesta extendería la protección a situaciones donde la conducta genera un peligro concreto para bienes jurídicos colectivos de primer orden —salud pública, seguridad ciudadana— sin exigir como elemento típico la específica consecuencia de movilización de servicios de emergencia, que constituye una restricción excesiva del ámbito de protección.

El artículo 510 del Código Penal, que tipifica los delitos de odio, fue identificado como otro precepto susceptible de valorar modificaciones.

No obstante, se estudió la posibilidad de introducir circunstancias agravantes específicas cuando las conductas tipificadas en el artículo 510 se realicen en el contexto de campañas coordinadas con financiación o dirección extranjera, o cuando se empleen medios técnicos de amplificación artificial —redes de *bots*, compra de tendencias— que multipliquen exponencialmente el alcance del discurso de odio. Estas agravantes reconocerían que la mayor antijuricidad deriva no solo del contenido del mensaje sino de los medios empleados para su difusión masiva y de su inserción en operaciones orquestadas. Sin embargo, varios participantes expresaron cautelas sobre esta línea de reforma, señalando que podría generar complejidades probatorias adicionales y que el régimen punitivo del artículo 510 ya contempla penas significativas.

Ámbito electoral

La necesidad de reforma de la legislación electoral para adaptarla a las realidades de la comunicación política digital y para tipificar específicamente la injerencia extranjera en procesos electorales mediante conductas inauténticas y coordinadas concitó un consenso particularmente robusto entre los participantes. La Ley Orgánica del Régimen Electoral General (LOREG) fue caracterizada de forma unánime como "desfasada" y "que no responde a la realidad digital".

Los expertos señalaron que la LOREG contiene un régimen detallado de prohibiciones y obligaciones sobre propaganda electoral, pero estas disposiciones fueron concebidas cuando la comunicación política se canalizaba fundamentalmente a través de medios tradicionales —prensa, radio, televisión— operando en territorio nacional y sujetos a marcos regulatorios específicos. Las normas sobre períodos de reflexión, prohibiciones de difusión de encuestas, limitaciones a la publicidad electoral, resultaban operativas en ese contexto. Sin embargo, la migración del debate político hacia plataformas digitales globales, la emergencia de "micromedios"[5], la relevancia de influencers, y la posibilidad de microsegmentación mediante publicidad programática, han tornado estas disposiciones crecientemente insuficientes.

[5] Agentes o canales informativos que operan en el ecosistema digital con capacidad de influencia significativa, pero que no están sujetos a las mismas obligaciones y responsabilidades que los medios de comunicación

La propuesta consensuada establece la necesidad de emprender una reforma integral de la LOREG que incluya la tipificación como infracción —con naturaleza administrativa o incluso penal según la gravedad— de la injerencia electoral por parte de actores estatales extranjeros o sus intermediarios mediante conductas inauténticas y coordinadas. Esta tipificación debería capturar diversos supuestos: financiación encubierta de campañas electorales por gobiernos extranjeros o entidades controladas por estos, despliegue de redes de cuentas falsas coordinadas que amplifican artificialmente determinadas opciones políticas o generen percepciones distorsionadas sobre el estado de la opinión pública, difusión masiva de contenidos falsos durante el período electoral mediante infraestructuras operadas desde el extranjero, y suplantación de candidaturas, partidos o instituciones electorales para difundir información falsa, principalmente sobre el proceso de votación.

Los participantes enfatizaron que esta tipificación debería inspirarse en el derecho comparado, mencionándose específicamente las reformas implementadas en Reino Unido, Francia, Dinamarca y California (Estados Unidos). Reino Unido aprobó una nueva ley de seguridad nacional en 2023[6], que incluye una definición de conductas que constituyen "injerencia" y tipifica injerencias electorales en beneficio o bajo influencia extranjera. Francia reformó su código electoral incorporando disposiciones específicas sobre desinformación en contexto electoral[7]. Dinamarca modificó su código penal (art. 108) para tipificar la cooperación con servicios de inteligencia extranjeros para llevar a cabo actividades de injerencia con el fin de influir en la toma de decisiones o en la formación de la opinión pública y ha presentado un proyecto de reforma[8] de la Ley de Propiedad Intelectual para regular *deepfakes* bajo ciertas circunstancias. California aprobó legislación específica[9] sobre *deepfakes* en publicidad electoral. Estos referentes comparados demuestran que democracias consolidadas con protección robusta de libertades han considerado viable y necesario establecer marcos sancionadores específicos para injerencias, incluidas las electorales, sugiriendo que España mantiene un déficit regulatorio en este ámbito.

La técnica legislativa propuesta requeriría definir con precisión varios elementos: qué se entiende por "actor estatal extranjero" —incluyendo no solo gobiernos sino entidades controladas—, qué constituye "conducta inauténtica" —comportamiento coordinado mediante cuentas falsas, ocultación de autoría, suplantación de identidades—, cuál es

---

[6] https://www.legislation.gov.uk/ukpga/2023/32/contents

[7] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847711/
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000049571951

[8] https://www.ft.dk/samling/20241/almdel/kuu/bilag/232/3050901.pdf

[9] https://law.justia.com/codes/california/code-elec/division-20/chapter-1/section-20012/
https://law.justia.com/codes/california/code-elec/division-20/chapter-7/section-20513/

el umbral de "coordinación" necesario para la tipicidad, y qué bienes jurídicos específicos se protegen —integridad del proceso electoral, libertad de formación de voluntad de los electores, igualdad de oportunidades entre opciones políticas. La definición precisa de estos elementos resulta indispensable para satisfacer las exigencias constitucionales de taxatividad y para evitar que la tipificación pueda ser instrumentalizada para restringir participación legítima en debates electorales.

Los participantes señalaron que la tipificación electoral presenta ventajas dogmáticas específicas respecto a la creación de tipos penales generales sobre desinformación. El contexto electoral constituye un marco temporalmente acotado —desde la convocatoria hasta la proclamación de resultados— donde concurren intereses constitucionales cualificados que justifican restricciones más intensas a libertades ordinarias. La jurisprudencia constitucional ha reconocido que durante perío ds electorales resultan legítimas limitaciones a libertades que resultarían desproporcionadas en contextos ordinarios, precisamente porque se protege un bien jurídico de máxima relevancia: la integridad de los procesos de formación democrática de la voluntad popular. Esta doctrina proporciona un fundamento constitucional más sólido para la intervención punitiva en contexto electoral que el que existiría para sancionar desinformación en contextos no electorales.

Adicionalmente, la tipificación electoral permitiría establecer medidas cautelares específicas adaptadas a la urgencia temporal que caracteriza estos procesos. Los participantes señalaron que, durante campañas electorales, la difusión de desinformación en los días inmediatamente previos a la votación puede resultar especialmente lesiva, pues no existe tiempo material para refutaciones efectivas basadas en datos y hechos empíricos.

No obstante, según alguno de los expertos, deberían establecerse marcos de actuación dentro del Reglamento (UE) 2024/900 sobre transparencia y segmentación en la publicidad política, respecto su considerando número 20, para evitar la inserción de publicidad política que contenga desinformación.

RESPUESTA JURÍDICA: ANÁLISIS DE LA VÍA ADMINISTRATIVA

Fundamentación de la primacía del modelo administrativo

El análisis técnico-jurídico desarrollado por el grupo de discusión converge hacia una conclusión categórica: la intervención administrativa constituye el instrumento más idóneo para la neutralización de operaciones FIMI, superando las limitaciones inherentes a la aproximación penal.

Esta conclusión deriva de tres premisas fundamentales que articulan la preferencia sistémica por mecanismos administrativos:

- **1ª) Imperativo de celeridad procedimental**. La eficacia temporal constituye un requisito constitutivo, no accidental, de cualquier respuesta institucional a operaciones FIMI. La velocidad de propagación de estas campañas —potenciada la instrumentalización de los algoritmos de las plataformas y arquitecturas de viralización— impone umbrales de actuación incompatibles con los plazos procesales penales. La consumación del daño, en ocasiones irreparable (erosión reputacional, interferencia electoral, desestabilización institucional), antecede sistemáticamente a la respuesta judicial punitiva, limitando el contenido útil cualquier sanción *ex post facto*.

- **2ª) Inadecuación de los umbrales de tipicidad penal.** Las operaciones FIMI se caracterizan por su naturaleza agregativa: conductas individualmente atípicas que, coordinadas sistemáticamente, generan efectos lesivos para bienes jurídicos colectivos. El principio de legalidad penal (*nullum crimen sine lege stricta*) impide la construcción de tipos penales suficientemente flexibles para capturar patrones de comportamiento coordinado sin incurrir en indeterminación proscrita constitucionalmente. La vía administrativa permite regular estos fenómenos agregados, manteniendo garantías de certeza jurídica proporcionadas a la naturaleza de las intervenciones.

- **3ª) Optimización del equilibrio proporcionalidad-eficacia.** El modelo administrativo con control judicial *ex ante* permite articular un sistema de ponderación entre bienes jurídicos (seguridad nacional, integridad democrática versus libertad de expresión) que, incorporando garantías jurisdiccionales reforzadas, alcanza niveles de efectividad superiores a los mecanismos puramente penales o a intervenciones administrativas sin contrapesos judiciales.

Se insistió, no obstante, en que la vía administrativa tiene límites difícilmente traspasables, y que la intervención sancionadora relacionada con actos de expresión debe seguir siendo una competencia estrictamente judicial.

Análisis normativo de la Ley 34/2002 (LSSI)

La Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico constituye el sustrato normativo sobre el cual edificar el mecanismo propuesto. Los artículos 8 a 17 establecen un régimen de responsabilidad e intervención que, pese a su concepción pre-FIMI, contiene elementos estructurales aprovechables.

Contexto jurídico de referencia:

Artículo 8 LSSI. Este precepto articula una cláusula de responsabilidad general fundamentada en la protección de bienes jurídicos esenciales. La enumeración no exhaustiva (seguridad nacional, defensa, orden público, protección de menores) permite subsumir conceptualmente las amenazas FIMI bajo la categoría "orden público" o "seguridad nacional", interpretadas expansivamente. Sin embargo, la antigüedad de la formulación normativa genera incertidumbres hermenéuticas sobre su aplicabilidad a fenómenos contemporáneos no previstos por el legislador histórico.

Régimen de exención de responsabilidad (LSSI/Directiva 2000/31/CE): La LSSI transpone el modelo de la Directiva mediante exenciones tasadas y condicionadas para actividades de intermediación: mera transmisión y acceso (art. 14), copia temporal (art. 15), alojamiento/hosting (art. 16) y enlaces y buscadores (art. 17). La exención opera cuando el intermediario no origina la transmisión ni selecciona o modifica datos (arts. 14–15) y, para hosting y enlaces, carece de "conocimiento efectivo" de ilicitud y actúa con diligencia para retirar o inutilizar el acceso en cuanto lo adquiere. A efectos de la concurrencia del conocimiento efectivo, en relación con la jurisprudencia tradicional de la Sala Primera del TS, no resulta imprescindible que se haya dictado una resolución por órgano competente y que dicha resolución haya sido comunicada al servicio de almacenamiento o enlace, sino que el conocimiento de la irregularidad del material que se almacena o al que se enlaza puede obtenerse por cualesquiera otros medios, así mediante una notificación fehaciente y fundamentada de la parte afectada o incluso por la mera constancia de la ilicitud cuando sea evidente por sí misma. Este esquema se articula junto con la ausencia de una obligación general de supervisión derivada de la Directiva, y se complementa —no se sustituye— con el deber de ejecutar órdenes singulares de retirada o interrupción dictadas por autoridad competente (art. 11), con garantías de proporcionalidad y tutela judicial cuando proceda.

Valoración crítica del modelo LSSI

El modelo LSSI presenta ventajas estructurales significativas que justifican su selección como marco de referencia:

- Ventaja sistémica. La existencia de un procedimiento legalmente establecido reduce costes de transacción legislativa y riesgos de inseguridad jurídica transitoria. La estrategia de desarrollo normativo incremental sobre marcos existentes resulta preferible, desde criterios de economía legislativa y coherencia sistemática, a la construcción *ex nihilo* de nuevos regímenes.

- Ventaja garantista. La incorporación ya prevista del control jurisdiccional para afectaciones de derechos fundamentales constituye un elemento diferencial. Este mecanismo de validación judicial *ex ante* representa un modelo de intervención bifásica (administrativa-judicial) que optimiza la ponderación entre eficacia operativa y garantías constitucionales.

- Ventaja de compatibilidad europea. El fundamento de la LSSI en la Directiva 2000/31/CE y su potencial articulación con el Reglamento (UE) 2022/2065 (DSA) facilitan la coherencia multinivel del ordenamiento, evitando fragmentaciones entre el régimen nacional y el europeo.

No obstante, el marco presenta déficits estructurales que condicionan su operatividad:

- Déficit temporal. La obsolescencia tecnológica de una norma promulgada en 2002 genera desajustes entre supuestos de hecho regulados y realidades tecnológicas contemporáneas. El ecosistema digital actual —caracterizado por plataformas globales, algoritmos de recomendación, redes sociales de gran escala— difiere radicalmente del contexto normativo originario.

- Déficit de concreción. La ambigüedad en la delimitación de los supuestos habilitantes genera incertidumbre aplicativa. La cuestión hermenéutica central —si el artículo 17 LSSI permite intervenciones basadas en afectaciones a bienes jurídicos colectivos o se circunscribe a lesiones de derechos individuales— permanece sin resolución jurisprudencial consolidada.

- Déficit orgánico. La referencia genérica a "autoridad competente" sin designación específica constituye una laguna procedimental que impide la aplicación material del régimen. Esta indefinición no es meramente técnica sino constitutiva: sin autoridad competente designada, el procedimiento resulta inoperante. Algunos expertos proponen la designación explícita del organismo (CNMC también como candidata probable) que tendrá la potestad para iniciar estos procedimientos.

- Déficit procedimental. La ausencia de desarrollo específico para amenazas FIMI —indicadores de detección, plazos máximos en situaciones críticas, mecanismos de coordinación interinstitucional— configura un vacío regulatorio que requiere complementación normativa.

La superación de estos déficits requiere una estrategia legislativa dual que se analizará en el apartado 4.4., que incluye la reforma de la LSSI y la elaboración de una norma complementaria de desarrollo, designando la autoridad competente.

Requisitos de legitimidad

Se identificaron cuatro condiciones de legitimidad que operan como requisitos *sine qua non* del sistema. Estos requisitos no constituyen preferencias de diseño sino exigencias constitucionales implícitas derivadas del principio de proporcionalidad y de la garantía institucional de independencia judicial y administrativa.

La autonomía e independencia real (no meramente formal) de la autoridad administrativa constituye requisito constitutivo de legitimidad, lo que evita la instrumentalización política de competencias sobre contenidos.

La exigencia de criterios taxativos deriva del principio de legalidad administrativa y del mandato de certeza jurídica. La formulación "que esa autoridad administrativa aplique una normativa taxativa" expresó frustración ante situaciones donde autoridades deben "solucionar temas sin normativa".

La taxatividad no significa rigidez absoluta —la naturaleza evolutiva de las amenazas requiere cierta flexibilidad adaptativa— pero sí exige que los márgenes de discrecionalidad administrativa resulten previsibles y controlables jurisdiccionalmente.

La exigencia de "que si tiene que intervenir el juez, que intervenga de forma muy ágil" no constituye mera aspiración de eficiencia sino requisito de efectividad del derecho a la tutela judicial. Un control judicial que llega tarde equivale a ausencia de control, porque la medida administrativa se ejecuta de facto antes de su validación judicial.

La agilidad judicial requiere no solo voluntarismo sino ingeniería procedimental específica: predeterminación de trámites, eliminación de dilaciones estructurales, centralización competencial, habilitación de medios telemáticos, establecimiento de plazos imperativos con consecuencias jurídicas del incumplimiento.

La DSA para combatir la FIMI

El DSA incorpora instrumentos normativos significativos para la neutralización de operaciones FIMI, aunque su efectividad permanece condicionada a la acomodación de la legislación interna a las exigencias del Reglamento europeo.

Contexto jurídico de referencia:

- **Artículo 9 DSA. Órdenes de actuación contra contenidos ilícitos.** Establece que autoridades judiciales o administrativas nacionales pueden emitir órdenes dirigidas a prestadores de servicios intermediarios para actuación contra contenidos ilícitos específicos. Estas órdenes deben satisfacer requisitos de motivación, especificidad y proporcionalidad.

  La utilidad de este instrumento para FIMI resulta limitada porque las operaciones suelen integrarse por contenidos que, analizados individualmente, pudieran considerarse lícitos. Solo cuando la campaña incorpore elementos efectivamente ilícitos (suplantaciones constitutivas de delito, contenidos que incurran en tipos penales) el artículo 9 resulta directamente aplicable.

- **Artículo 18. Notificación de sospechas de delitos**. Cuando el prestador de servicios "tenga conocimiento de cualquier información que le haga sospechar que se ha cometido, se está cometiendo o es probable que se cometa un delito que implique una amenaza para la vida o la seguridad de una o más personas, comunicará su sospecha de inmediato a las autoridades policiales o judiciales del Estado miembro".

- **Artículos 34-35 DSA.** Gestión de riesgos sistémicos. Las plataformas de muy gran tamaño tienen obligación de identificar, analizar y mitigar riesgos sistémicos que sus servicios pueden generar. El catálogo de riesgos sistémicos incluye expresamente "efectos adversos reales o previsibles para los procesos electorales, el discurso cívico y los procesos electorales, así como para la seguridad pública".

  Este régimen permite actuación indirecta contra las campañas FIMI. La DSA habilita a obligar a las plataformas a implementar sistemas de mitigación de riesgos. Los coordinadores nacionales pueden supervisar adecuación de estos sistemas y, detectando insuficiencias, exigir medidas correctoras que, indirectamente, dificulten operaciones FIMI (mejores sistemas de detección de bots, transparencia de financiación de contenidos patrocinados, herramientas de autenticación de identidad).

- **Artículo 40 DSA.** Régimen de acceso a datos / investigadores autorizados. Los coordinadores nacionales pueden exigir a plataformas de muy gran tamaño acceso a datos cuando resulte necesario para evaluación de cumplimiento del reglamento. Esta facultad resulta instrumental para detección de comportamientos coordinados inauténticos, ya que estos patrones solo emergen mediante análisis agregados de datos no disponibles públicamente (metadatos de origen geográfico, análisis de redes de interacción, patrones temporales de actividad o análisis de propagación viral).

  La efectividad de este instrumento depende críticamente de la capacidad técnica del coordinador para procesar y analizar grandes volúmenes de datos, requiriendo inversión en infraestructura analítica.

- **Código de conducta reforzado contra la desinformación.** El DSA incorpora este código como instrumento de corregulación, convirtiendo compromisos voluntarios en obligaciones jurídicamente exigibles para signatarios. El incumplimiento del código puede considerarse elemento de valoración en evaluación de suficiencia de medidas de mitigación de riesgos.

Estrategia de integración LSSI-DSA

La recomendación técnica propone **utilizar el modelo LSSI como arquitectura procedimental para implementación nacional del DSA**, generando sistema integrado que unifique respuestas nacionales (LSSI) y europeas (DSA) bajo procedimientos comunes.

La materialización de esta estrategia requiere actuación normativa coordinada en cuatro niveles:

- **Nivel 1. Reforma LSSI**. Actualización integral del articulado para adaptación al ecosistema digital contemporáneo, incorporando explícitamente amenazas FIMI y definiendo comportamientos coordinados inauténticos como supuestos habilitantes cuando amenacen bienes jurídicos protegidos (seguridad nacional, integridad electoral, orden público).

- **Nivel 2. Ley de desarrollo de la DSA**. Norma específica que designe formalmente al coordinador nacional, donde se establezca su estructura organizativa, defina el cuadro completo de infracciones y sanciones (el DSA establece máximos, pero permite modulación nacional), y remita al procedimiento LSSI para actuaciones sobre contenidos.

  A esos efectos, pudiera servir de modelo la técnica utilizada en el proyecto de Ley para la protección de los menores en el entorno digital, actualmente en trámite en el Congreso de Diputados. A dicho fin, el proyecto propone la reforma del artículo 164 de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual[10]; del art 95 de la LOPJ y del artículo 122 bis de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

- **Nivel 3. Desarrollo reglamentario** al objeto de concretar aspectos técnicos: indicadores objetivables de detección de comportamientos coordinados (basados en análisis forense digital), protocolos de coordinación interinstitucional, mecanismos de colaboración con verificadores independientes (*fact-checkers* acreditados), sistemas de transparencia y rendición de cuentas.

---

[10] Esta Ley fue señalada por alguno de los expertos participantes en la discusión, como mecanismo que puede habilitar en el futuro respuestas para combatir las campañas FIMI, con modificaciones que obliguen expresamente a la adopción de medidas de mitigación de riesgos; que incorporen mecanismos de evaluación de riesgos de seguridad nacional para prestadores establecidos en terceros países; o que incluyan más acciones de transparencia para prestadores en relación con los "Usuarios de Especial Relevancia", cuando se constate, mediante indicios suficientes, su connivencia con actores estatales hostiles, y desplieguen o faciliten, en territorio nacional, campañas FIMI orquestadas por aquellos.

Designación de la autoridad competente: Análisis institucional

Las funciones de garantía atribuidas al coordinador de servicios digitales -la CNMC ha sido designada como entidad responsable de la supervisión y la aplicación de la DSA- actualmente están condicionadas a la acomodación legislativa antes referida. La mera expectativa o previsión administrativa resulta insuficiente. Se requiere base legal que atribuya formalmente competencias, defina procedimientos y establezca límites de actuación.

El modelo propuesto contempla que esta autoridad disponga de:

- Facultades de monitorización. Acceso a datos agregados de plataformas que permitan detectar anomalías en patrones de comportamiento. Esta facultad debe articularse respetando los límites constitucionales de protección de datos personales, requiriendo probablemente el establecimiento de mecanismos de anonimización o seudonimización que preserven privacidad individual mientras permiten análisis agregados. Además, habría que garantizar la no intromisión en otros derechos fundamentales, como la intimidad y el secreto de las comunicaciones.

- Potestades de investigación. Capacidad de requerir información específica a plataformas cuando indicios suficientes sugieran la existencia de campañas coordinadas. Esta potestad debe ejercerse mediante resoluciones motivadas que especifiquen el objeto, alcance y plazo de la información requerida.

- Competencia decisoria. Facultad de adoptar resoluciones, como autoridad independiente y, en sus funciones de supervisión, requiriendo a las plataformas la ejecución de las medidas a las que están obligadas por la diversa regulación comentada, como la retirada de contenidos o la reducción de riesgos sistémicos, sujetas a requisitos de motivación reforzada y control jurisdiccional previo cuando afecten libertades comunicativas.

- Capacidad y recursos técnicos que hagan efectivas las competencias descritas y las labores de coordinación y colaboración entre los organismos implicados, que apoye y oriente a la autoridad en el ejercicio de sus facultades.

CONCLUSIONES Y RECOMENDACIONES

Las Operaciones de Manipulación e Injerencia Extranjera de la Información (FIMI) representan una amenaza estructural para la soberanía democrática, y nuestro ordenamiento actual es manifiestamente insuficiente para neutralizarla. La clave conceptual, y el principal desafío para el legislador, radica en comprender que la amenaza FIMI no reside en la falsedad del contenido per se, sino en el patrón de comportamiento coordinado, intencional y sistemático desplegado por actores estatales. Nuestros sistemas legales, diseñados para sancionar actos individuales y contenidos ilícitos, se muestran impotentes ante operaciones que basan su toxicidad en la orquestación y la amplificación artificial, donde las piezas individuales de contenido, aisladamente, suelen ser consideradas lícitas.

Esta obsolescencia normativa es transversal. El Derecho Penal, si bien debe ser reformado quirúrgicamente para tipificar conductas habilitantes, como la suplantación de identidad, es una herramienta estructuralmente inadecuada para la respuesta inmediata que exige la FIMI. Sus problemas de territorialidad y atribución, sumados a una temporalidad incompatible con la velocidad de las crisis informativas, lo descartan como solución primaria. De igual modo, la legislación electoral (LOREG) evidencia un desfase anacrónico con la realidad de las campañas digitales. Mientras tanto, instrumentos europeos potentes como DSA permanecen infrautilizados por la inacción en el desarrollo normativo nacional y la falta de acomodación de la legislación interna a las exigencias del Reglamento europeo.

En consecuencia, el consenso técnico apunta de forma sólida hacia la vía administrativa como el instrumento más ágil y efectivo, siempre y cuando se articule sobre una arquitectura de garantías robusta. Una actualización de la LSSI ofrece una base procedimental, pero su eficacia dependerá críticamente de cuatro pilares inexcusables: la autonomía funcional e independencia del órgano supervisor respecto del poder ejecutivo; la taxatividad normativa en la definición de los supuestos de intervención (qué es exactamente "comportamiento coordinado inauténtico"); la proporcionalidad estricta en las medidas que, en cada caso pueden adoptarse (diferenciando la retirada de contenido del cierre de un canal o bloqueo de un dominio); y, de forma crucial, la implementación de un mecanismo de validación judicial ágil, para equilibrar la respuesta rápida con la salvaguarda de derechos fundamentales.

Paralelamente, la regulación debe extenderse más allá de la acción estatal y abordar el ecosistema que facilita la injerencia. Es imperativo exigir a las grandes plataformas (VLOPs) una transparencia algorítmica auditable, obligar al etiquetado de contenidos sintéticos (IA/*deepfakes*) y forzar la eliminación proactiva de redes de bots coordinados. Asimismo, la

aparición de "usuarios de especial relevancia" (*influencers*) con audiencias masivas exige la creación de un registro y obligaciones de transparencia financiera, especialmente ante financiación proveniente de entidades extranjeras opacas, equiparando parcialmente sus responsabilidades a las de los medios tradicionales cuando su actividad principal es la difusión de información.

Ninguna reforma legal será efectiva sin una voluntad política sostenida, inmune a la polarización electoral, y sin una inversión decisiva en capacidades técnicas y humanas. La lucha contra la FIMI exige una coordinación interinstitucional real, cooperación internacional reforzada (especialmente frente a plataformas no cooperativas) y una apuesta estratégica a largo plazo por la alfabetización mediática de la ciudadanía, siguiendo los modelos de resiliencia social probados en países como Finlandia o Estonia. Nos enfrentamos a un desafío dinámico, y nuestra respuesta debe ser igualmente sofisticada, ágil y, sobre todo, democráticamente garantista.

Finalmente, Estrategia Nacional contra las Campañas de Desinformación, actualmente en proceso de elaboración, puede ser la base para articular líneas de acción que, de acuerdo a la experiencia adquirida, mejoren los mecanismos de coordinación existentes y, teniendo en cuenta los instrumentos analizados y aportados por la reciente legislación europea, faciliten una cooperación y comunicación reales y efectivas, fluidas y directas entre los representantes de los distintos organismos implicados mencionados, con una vocación de permanencia que permita establecer sinergias, especialmente en los momentos más críticos.