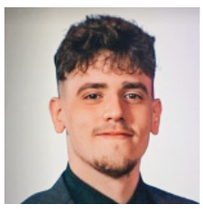
DOCTRINA

Cyber deception y operaciones de influencia extranjera
El desafío de la desinformación patrocinada por los Estados

por Tomás Illuminati Balbín(*) y Facundo Nahuel Britos(**)



Sumario: I. Introducción: el caso "La Compañía" y la doble cara del engaño. – II. *Cyber deception*: dos acepciones a distinguir. – III. El ecosistema ruso de desinformación. – IV. El caso "La Compañía": anatomía de una operación. – V. Marcos normativos comparados: Argentina, Estados Unidos, Unión Europea y OTAN. – VI. Conclusiones y recomendaciones. – VII. Bibliografía.

I. Introducción: el caso "La Compañía" y la doble cara del engaño

En abril de 2026, un consorcio internacional de medios reveló que presuntamente una estructura de influencia conocida internamente como "La Compañía" (en inglés, "The Company") habría operado en la Argentina durante el año 2024, con un objetivo declarado, desacreditar la política exterior proucraniana del gobierno argentino[1]. La investigación, coordinada por la organización Forbidden Stories, partió de 76 documentos filtrados (1.431 páginas en idioma ruso) obtenidos por el medio africano *The Continent* y compartidos con un grupo de medios que incluyó a openDemocracy (Reino Unido), iStories y Dossier Center (Rusia), All Eyes on Wagner (Francia) y Filtraleaks (Argentina)[2]. Según esos textos, la operación habría presupuestado al menos doscientos ochenta y tres mil cien dólares estadounidenses (USD$283.100) para "inyectar" alrededor de 250 artículos críticos del gobierno argentino en no menos de 23 portales digitales locales, entre junio y octubre de 2024, con pagos de entre USD$350 y USD$3100 por nota, más otros USD$343.000 destinados a recolección de inteligencia, encuestas y perfiles de figuras públicas[3].

Las tácticas atribuidas a la red resultan ilustrativas de lo que la doctrina especializada denomina engaño informativo. Los documentos describen la creación de "periodistas" y "expertos" inexistentes, entre ellos, un tal "Manuel Godsin", cuya fotografía pertenecía en realidad a un ciudadano ruso y cuyas credenciales académicas (un supuesto doctorado por la Universidad de Bergen) no pudieron ser verificadas, el uso de contenido generado o asistido por inteligencia artificial, la difusión de noticias directamente fabricadas (entre ellas, una historia sobre un presunto "grupo de sabotaje" enviado por el gobierno argentino para atacar un gasoducto con Chile, catalogada internamente con el objetivo de "crear tensión entre Argentina y Chile"); y pagos a cuentas de personas influyentes (*influencers*) en redes sociales[4].

El episodio tiene resonancia política y jurídica. Las preguntas concretas que surgen serían: ¿puede el Estado argentino sancionar la manipulación informativa coordinada por una potencia extranjera sin lesionar la libertad de expresión? ¿Existen tipos penales aplicables a la suplantación de identidad mediante personas ficticias o a los pagos encubiertos? ¿Debe la Argentina seguir el modelo regulatorio de la Unión Europea, el modelo de exposición y sanciones de los Estados Unidos, o abstenerse? Antes de responder conviene observar a fondo una ambigüedad conceptual que va más allá de todo el problema, la del término *cyber deception* (engaño cibernético), que designa dos fenómenos opuestos.

II. *Cyber deception*: dos acepciones a distinguir

El concepto militar de engaño (*deception*) ingresó al vocabulario de la ciberseguridad con dos sentidos que conviene no confundir, porque uno es una herramienta lícita de defensa y el otro es, precisamente, la amenaza que se busca combatir.

En su acepción defensiva, el *cyber deception* designa la colocación deliberada de activos informáticos falsos para detectar, desviar y estudiar a los atacantes. La definición per se del señuelo, o *honeypot*, pertenece a Lance Spitzner, quien lo definió como "un recurso de seguridad cuyo valor reside en ser sondeado, atacado o comprometido"[5]. El glosario técnico, explicado en términos accesibles, distingue el *honeypot* (un sistema señuelo completo que imita un activo real, de modo que todo acceso resulta sospechoso por diseño), el *honeytoken* (un dato falso, una credencial o un archivo, que dispara una alerta al ser utilizado) y la *honeynet* (una red entera de señuelos). Estas técnicas están normalizadas en estándares oficiales, el control SC-26 del Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST), titulado "Decoys" (Señuelos) en la Revisión 5 de su Publicación Especial 800-53 (denominado "Honeypots" en la revisión anterior), ordena incluir componentes diseñados específicamente para ser blanco de ataques, a fin de detectar, desviar y analizar tales ataques[6].

Nota de Redacción: Sobre el tema ver, además, los siguientes trabajos publicados en El Derecho: *Derecho al olvido en Internet*, por Hugo Alfredo Vaninetti, ED, 242-566; *Derecho al olvido en materia disciplinaria laboral*, por Pablo Mosca, EDLA, 2011-B-1155; *La neutralidad y la libertad de expresión e información en Internet*, por Hugo Alfredo Vaninetti, ED, 246-745; *El derecho al olvido en Internet (un fallo del Tribunal de Justicia de la Unión Europea que contribuye a la preservación de la imagen en los entornos virtuales)*, por Guillermo F. Peyrano, ED, 258-918; *La responsabilidad de las entidades financieras y el "derecho al olvido" de la ley de hábeas data*, por Carlos Enrique Llera, ED, 260-624; *La protección de los datos personales en Internet: lineamientos que caben deducirse del fallo de la Corte Suprema*, por Esteban Ruiz Martínez, ED, 260-861; *El miedo a Internet*, por Gregorio Badeni, ED, 265-616; *Los diarios online como legitimados pasivos del derecho al olvido. Diferencias entre la Casación belga y la Casación francesa*, por Pablo A. Palazzi, ED, 269-519; *Difusión no autorizada de imágenes íntimas (revenge porn)*, por Pablo A. Palazzi, ED, 266-837; *Derecho a la privacidad y protección de datos personales en las condiciones de uso y políticas de privacidad de las redes sociales*, por John Grover Dorado, ED, 268-609; *El debate del derecho al olvido en el Brasil*, por Aislan Vargas Basilio, ED, 273-808; *El derecho al olvido en Internet frente a la libertad de expresión*, por Verónica Elvia Melo, ED, 288-968; *Las noticias falsas ("fake news"), posverdad, democracia y la libertad de expresión en internet*, por Hugo Alfredo Vaninetti, ED, 289-1168; *"Netchoice vs. Paxton" (o los desafíos de internet y la libertad de expresión)*, por Enrique H. Del Carril, ED, 297; *Combatiendo la desinfodemia: herramientas de diagnóstico y respuestas recientes al recrudecimiento de los conflictos entre la libertad de expresión y los derechos individuales y colectivos ante las fake news*, por Oscar R. Puccinelli, Derecho, Innovación & Desarrollo Sustentable, Número 9 - octubre 2022. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(*) Cyber Security Analyst, Threat Intelligence Specialist, MSc in Cyber Security Candidate at Open University (UK), OWASP Rosario Chapter Leader, Vulnerability Researcher, x6 CVEs reconocidos en MITRE, Miembro de IALEIA.

(**) Licenciado en Relaciones Internacionales (UAI). OWASP Rosario Chapter Leader. Moderador y expositor en espacios académicos y profesionales vinculados a la ciberseguridad y la ciberdiplomacia.

(1) Diana Cariboni, "Russia Tried to Discredit Milei in Argentina, but Ended Up Damaging Its Media Instead", *openDemocracy*, mayo de 2026, https://www.opendemocracy.net/russia-tried-to-discredit-milei-in-argentina-but-ended-up-damaging-its-media-instead/

(2) Forbidden Stories, "Propaganda Machine: Secret Documents Reveal Russia's Foreign Influence Strategy Across Three Continents", *Forbidden Stories*, abril de 2026, https://forbiddenstories.org/propaganda-machine-secret-documents-reveal-russias-foreign-influence-strategy-across-three-continents/

(3) MercoPress, "Leak Reveals Russian Campaign to Discredit Milei Through Argentine Media Outlets", *MercoPress*, 4 de abril de 2026, https://en.mercopress.com/2026/04/04/leak-reveals-russian-campaign-to-discredit-milei-through-argentine-media-outlets

(4) Diana Cariboni, Sofía Álvarez Jurado y Santiago O'Donnell, "Leña al fuego: La campaña rusa para influir en los medios de comunicación de Argentina", *openDemocracy*, 2 de abril de 2026, https://www.opendemocracy.net/es/argentina-rusia-propaganda-medios-periodismo-milei-ucrania-putin-trump-prigozhin/

(5) Lance Spitzner, *Honeypots: Tracking Hackers* (Boston: Addison-Wesley Professional, 2002). A Spitzner se atribuye, además, la acuñación del término *honeytoken*.

(6) National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publication 800-53, Revisión 5, septiembre de 2020, https://doi.org/10.6028/NIST.SP.800-53r5

A su vez, la Publicación Especial 800-160, Volumen 2, Revisión 1, del propio NIST incorpora el engaño (*deception*) como una de sus técnicas de ciberresiliencia[7]. El marco operativo de referencia es MITRE Engage (sucesor de MITRE Shield y articulado con la matriz MITRE ATT&CK), cuyo glosario define el engaño (*deception*) como "revelar, ocultar o manipular de algún otro modo hechos y ficciones para inducir a error o confundir a un adversario, de modo que este actúe de una manera beneficiosa para quien lo engaña"[8]. La literatura académica revisada por pares ha sistematizado tres décadas de estas técnicas (señuelos, *honeytokens* y defensa de objetivo móvil) y su utilidad para interrumpir las distintas fases de un ataque[9].

En su acepción ofensiva, en cambio, el mismo concepto de engaño se aplica a la manipulación del entorno informativo de una sociedad. La Unión Europea acuñó para este fenómeno el término oficial de Manipulación e Interferencia de Información Extranjera (en inglés, *Foreign Information Manipulation and Interference*, FIMI), que el Servicio Europeo de Acción Exterior (EEAS) define como "un patrón de comportamiento que por lo general no es ilegal y que amenaza o tiene el potencial de impactar negativamente valores, procedimientos y procesos políticos", de carácter manipulador, conducido de manera intencional y coordinada por actores estatales o sus delegados. La Organización del Tratado del Atlántico Norte (OTAN), por su parte, emplea el concepto de "guerra cognitiva" (*cognitive warfare*), definido por su Mando Aliado de Transformación como "las actividades conducidas en sincronización con otros instrumentos de poder para afectar las actitudes y el comportamiento, influyendo, protegiendo o perturbando la cognición individual y grupal, a fin de obtener ventaja sobre un adversario". El glosario relevante incluye los *deepfakes* (vídeos o audios sintéticos hiperrealistas), los *bots* (cuentas automatizadas), las "granjas de troles" (*troll farms*, operadores que simulan ser ciudadanos comunes), la propaganda computacional (difusión algorítmica a gran escala) y los sitios *doppelganger* (clones de medios legítimos).

El puente conceptual entre ambas acepciones es que, en los dos casos, "engañar" significa inducir en el destinatario una representación falsa de la realidad. La diferencia es decisiva, en la defensa de redes, el engañado es el atacante y el engaño es lícito, en las operaciones de influencia, el engañado es el público de una democracia y el engaño es la amenaza. El derecho debe distinguir con nitidez ambos sentidos para no penalizar el primero al combatir el segundo. La dimensión del problema no es menor; el cuarto informe anual del EEAS, publicado en marzo de 2026, detectó y analizó quinientos cuarenta incidentes de FIMI durante el año 2025, de los cuales un 29 % fue atribuido a Rusia y un 6 % a China, con afectación de todas las regiones del mundo[10].

III. El ecosistema ruso de desinformación

El caso argentino, de confirmarse, no constituiría un hecho aislado, sino que se inscribiría como un nodo de un ecosistema de desinformación de origen ruso que ha sido documentado de manera independiente por gobiernos y organismos occidentales. Esta circunstancia refuerza la verosimilitud del patrón, aunque, como se verá, no sustituye la prueba del caso concreto.

La operación más conocida es "Doppelganger", una campaña de clonación de medios occidentales legítimos. El 4 de septiembre de 2024, el Departamento de Justicia de los Estados Unidos anunció la incautación de treinta y dos dominios de internet utilizados en esa campaña y la atribuyó a las compañías rusas Social Design Agency (SDA), Structura National Technology y ANO Dialog, operando bajo la dirección de la Administración Presidencial rusa, en particular del primer subjefe de gabinete Sergei Kiriyenko[11]. Con anterioridad, el 20 de marzo de 2024, la Oficina de Control de Activos Extranjeros del Tesoro estadounidense (OFAC) ya había sancionado a Ilya Gambashidze (fundador de la SDA) y a Nikolai Tupikin (de Structura) por implementar, en nombre del gobierno ruso, una red de más de sesenta sitios que suplantaron a organizaciones de prensa legítimas[12].

A esta operación se suma la red "Pravda" (también rastreada como "Portal Kombat"), un conjunto de agregadores de noticias prorrusas que, según la investigación conjunta del Laboratorio de Investigación Forense Digital del Atlantic Council (DFRLab) y la firma finlandesa CheckFirst, publicó más de tres millones setecientos mil artículos. A esta red se asocia, además, la técnica conocida como "amaestramiento de modelos de lenguaje" (*LLM grooming*), consistente en contaminar deliberadamente los datos con que se entrenan los sistemas de inteligencia artificial para que estos reproduzcan narrativas del Kremlin[13].

La organización europea EU DisinfoLab ha caracterizado a Doppelganger como "una de las operaciones de información rusas más emblemáticas desde el fin de la Guerra Fría"[14]. Ya en 2020, el Departamento de Estado de los Estados Unidos había sistematizado los cinco pilares de este ecosistema: las comunicaciones oficiales del gobierno, la mensajería estatal global (RT y Sputnik), el cultivo de fuentes delegadas, las redes sociales instrumentalizadas y la desinformación habilitada por medios cibernéticos[15].

IV. El caso "La Compañía": anatomía de una operación

Encuadrado en ese ecosistema, el caso argentino presenta rasgos totalmente propios. Según los documentos filtrados, "La Compañía" sería la sucesora operativa del Grupo Wagner de Yevgeny Prigozhin, cuyas operaciones de información en el exterior habrían pasado, tras la muerte de Prigozhin en 2023, al control de los servicios de inteligencia rusos. La campaña argentina habría coincidido con el período de mayor alineamiento de Buenos Aires con Washington y Kiev. Cabe consignar una divergencia de atribución no resuelta: mientras la investigación periodística vincula la estructura a una agencia de inteligencia, fuentes oficiales argentinas la asociaron a otra. La identificación precisa del servicio responsable debe asignársele, por ahora, baja confianza.

Resulta imprescindible subrayar las limitaciones probatorias que los propios investigadores reconocen, y que imponen tratar el caso como operación *presunta*. En primer lugar, los documentos no acreditan que los pagos se hayan efectivamente realizado ni a quién; en segundo lugar, algunos artículos aparecen duplicados en las planillas, y en tercer lugar, varias cifras podrían estar infladas, práctica que el investigador Maxime Audinet, citado por el consorcio, atribuye a la "corrupción endémica" del sistema de propaganda ruso[16].

La mayoría de los más de veinte medios mencionados negó haber recibido dinero. El investigador del Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), Martín Becerra, señaló, además, que el resultado de la operación fue "el opuesto al que en teoría se preten-

(7) Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau y Rosalie McQuaid, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, NIST Special Publication 800-160, Volumen 2, Revisión 1, diciembre de 2021, https://doi.org/10.6028/NIST.SP.800-160v2r1

(8) The MITRE Corporation, "MITRE Engage: Términos Clave (Glosario)", *MITRE Engage*, 2022, https://engage.mitre.org/learn-more-glossary/

(9) Li Zhang y Vrizlynn L. L. Thing, "Three Decades of Deception Techniques in Active Cyber Defense: Retrospect and Outlook", *Computers & Security* 106 (2021): 102288, https://doi.org/10.1016/j.cose.2021.102288

(10) European External Action Service, *4th EEAS Annual Report on Foreign Information Manipulation and Interference Threats*, marzo de 2026, https://www.eeas.europa.eu/eeas/4th-eeas-annual-report-foreign-information-manipulation-and-interference-threats_en

(11) U.S. Department of Justice, "Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere", *Office of Public Affairs*, 4 de septiembre de 2024, https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

(12) U.S. Department of the Treasury, "Treasury Sanctions Actors Supporting Kremlin-Directed Malign Influence Efforts", comunicado de prensa JY2195, 20 de marzo de 2024, https://home.treasury.gov/news/press-releases/jy2195

(13) Digital Forensic Research Lab (DFRLab) y CheckFirst, "Russia's So-Called 'Pravda' Network Expands Worldwide", *DFRLab*, 24 de febrero de 2025, https://dfrlab.org/2025/02/24/russia-pravda-network-expands-worldwide/

(14) EU DisinfoLab, "Doppelganger Hub", *EU DisinfoLab*, actualizado a 7 de julio de 2025, https://www.disinfo.eu/doppelganger-hub

(15) U.S. Department of State, Global Engagement Center, *GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem*, 5 de agosto de 2020, https://2017-2021.state.gov/russias-pillars-of-disinformation-and-propaganda-report/

(16) Forbidden Stories, "Ghost Journalists, Cash and Kremlin Scripts: How Russian Operatives Tried to Influence Argentinian Media", *Forbidden Stories*, 2 de abril de 2026, https://forbiddenstories.org/ghost-journalists-cash-and-kremlin-scripts-how-russian-operatives-tried-to-influence-argentinian-media/

día", dado que el partido gobernante se fortaleció en las elecciones legislativas posteriores, lo que sugiere que la finalidad real de estas campañas es "pescar en río revuelto", esto es, erosionar la confianza institucional más que obtener un resultado electoral determinado. La Embajada de Rusia en Buenos Aires calificó la investigación de material "infundado" (*baseless*).

En el plano de la respuesta estatal, en junio de 2025 el vocero presidencial Manuel Adorni anunció que la Secretaría de Inteligencia de Estado (SIDE) había detectado la red e identificado a un ciudadano ruso y su cónyuge como responsables locales, presuntamente vinculados al "Proyecto Lakhta", la misma estructura que los Estados Unidos asocian a la interferencia rusa desde 2016[17]. El Foro de Periodismo Argentino (FOPEA) había advertido ya en enero de 2026, en su informe sobre campañas de desinformación promovidas desde el exterior (elaborado con apoyo del Ministerio de Asuntos Exteriores de Polonia), acerca del ofrecimiento de pagos en criptomonedas a comunicadores locales y de la circulación de un *deepfake* de un diplomático extranjero[18]. Reportes posteriores a abril de 2026 mencionaron detenciones individuales que, al cierre de este trabajo, no pudieron confirmarse de forma independiente y que, por ende, no deben darse por establecidas.

V. Marcos normativos comparados: Argentina, Estados Unidos, Unión Europea y OTAN

El caso obliga a confrontar el derecho argentino con las respuestas que han ensayado otras jurisdicciones. Y el contraste mismo revela, ante todo, un vacío legal local.

En la Argentina, por ejemplo, no existe legislación específica contra la interferencia informativa extranjera, y el marco aplicable es fragmentario. La libertad de expresión goza de una protección reforzada, los artículos 14 y 32 de la Constitución Nacional, este último al prohibir al Congreso federal dictar leyes que restrinjan la libertad de imprenta o establezcan sobre ella la jurisdicción federal, y el artículo 13 de la Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica), incorporada con jerarquía constitucional por el artículo 75, inciso 22[19]. La Convención protege la libertad de expresión en su doble dimensión, individual y social, y proscribe la censura previa[20]. La doctrina de la Corte Interamericana de Derechos Humanos es categórica: en su Opinión Consultiva OC-5/85 estableció que las restricciones a la libertad de expresión deben ser "necesarias" para asegurar un fin legítimo, sin que baste con que sean meramente "útiles"[21].

En materia infraconstitucional, la Ley 25.326 de Protección de los Datos Personales tutela el dato personal y regula su tratamiento, incluso con fines de inteligencia[22], mientras que la Ley 26.388, que modificó el Código Penal, tipifica conductas como el acceso ilegítimo a sistemas informáticos (artículo 153 bis) y el fraude informático (artículo 173, inciso 16)[23]. En el plano institucional, el reciente Decreto de Necesidad y Urgencia 941/2025, que reformó la Ley de Inteligencia Nacional 25.520, creó (en disposición separada) el Centro Nacional de Ciberseguridad como organismo descentralizado en la órbita de la Secretaría de Innovación, Ciencia y Tecnología de la Jefatura de Gabinete de Ministros[24]. Ninguna de estas normas, sin embargo, aborda específicamente la manipulación informativa coordinada por un Estado extranjero.

El modelo estadounidense, por otro lado, históricamente basado en la exposición y las sanciones, atraviesa hoy un repliegue significativo. Su principal órgano federal contra la desinformación extranjera, el Global Engagement Center (GEC) del Departamento de Estado, cerró por caducidad legal el 23 de diciembre de 2024, al no renovarse su autorización en la ley de autorización de defensa (NDAA)[25]. El cierre, que afectó a una dependencia de aproximadamente ciento veinte empleados y sesenta y un millones de dólares (USD$61.000.000) de presupuesto anual, se debió en parte a acusaciones de censura del discurso doméstico, una tensión central para el jurista[26]. Subsisten, no obstante, herramientas como la Ley de Registro de Agentes Extranjeros (*Foreign Agents Registration Act*, FARA), que impone obligaciones de divulgación pública a quienes representan intereses de potencias extranjeras[27].

El bloque europeo, por su parte, ha desarrollado el modelo regulatorio más completo, centrado en la transparencia y la diligencia de las plataformas más que en la prohibición de contenidos. El Reglamento (UE) 2022/2065, o Ley de Servicios Digitales (*Digital Services Act*), impone a las plataformas en línea –de gran tamaño– obligaciones de evaluación y mitigación de riesgos sistémicos (incluida la desinformación), bajo multas de hasta el seis por ciento de su facturación global anual[28].

El Código de Buenas Prácticas en materia de Desinformación, de 2022, se integró formalmente al marco de la Ley de Servicios Digitales con efecto desde el 1 de julio de 2025, convirtiéndose en parámetro de cumplimiento auditable[29]. La Unión Europea adoptó medidas más drásticas mediante el Reglamento (UE) 2022/350 del Consejo, del 1 de marzo de 2022, que suspendió la difusión de los medios estatales rusos RT y Sputnik por cualquier vía, una medida que parte de la doctrina ha cuestionado por su tensión con la libertad de expresión y que ilustra el dilema jurídico de fondo[30].

En el plano técnico, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha analizado la FIMI desde una perspectiva técnica[31].

Y cabe destacar que la OTAN, finalmente, ha conceptualizado la amenaza en clave de seguridad colectiva. Su Mando Aliado de Transformación desarrolla el "Concepto de Guerra Cognitiva" antes citado, en el marco de una doctrina más amplia sobre amenazas híbridas, esto es, la combinación de medios convencionales y no convencionales por debajo del umbral del conflicto armado.

(17) Meduza, "Argentina Says It Uncovered Russian Spy Ring Suspected of Disinformation Efforts", *Meduza*, 19 de junio de 2025, https://meduza.io/en/news/2025/06/19/argentina-says-it-uncovered-russian-spy-ring-suspected-of-disinformation-efforts

(18) Foro de Periodismo Argentino (FOPEA), "Investigación de FOPEA revela los 'mecanismos invisibles' de la desinformación extranjera en Argentina", *FOPEA*, 20 de enero de 2026, https://fopea.org/investigacion-de-fopea-revela-los-mecanismos-invisibles-de-la-desinformacion-extranjera-en-argentina/

(19) Constitución de la Nación Argentina, arts. 14, 32 y 75, inc. 22. El art. 32 dispone que "el Congreso federal no dictará leyes que restrinjan la libertad de imprenta o establezcan sobre ella la jurisdicción federal".

(20) Organización de los Estados Americanos, *Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica)*, art. 13, San José, 22 de noviembre de 1969, https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm

(21) Corte Interamericana de Derechos Humanos, *La Colegiación Obligatoria de Periodistas (arts. 13 y 29 Convención Americana sobre Derechos Humanos)*, Opinión Consultiva OC-5/85 del 13 de noviembre de 1985, Serie A No. 5, https://www.corteidh.or.cr/docs/opiniones/seriea_05_esp.pdf

(22) Congreso de la Nación Argentina, "Ley 25.326, Protección de los Datos Personales", Boletín Oficial, 2 de noviembre de 2000, https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/actualizacion

(23) Congreso de la Nación Argentina, "Ley 26.388, Código Penal. Modificación", Boletín Oficial, 25 de junio de 2008, https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto

(24) Poder Ejecutivo Nacional, "Decreto 941/2025", *Boletín Oficial de la República Argentina*, 2 de enero de 2026, https://www.boletinoficial.gob.ar/detalleAviso/primera/337032/20260102. El decreto, firmado el 31 de diciembre de 2025, modificó la Ley de Inteligencia Nacional 25.520; su artículo 2 bis establece el carácter encubierto de la actividad de inteligencia nacional, mientras que la creación del Centro Nacional de Ciberseguridad se dispone en un artículo diferenciado.

(25) Congressional Research Service, "Termination of the State Department's Global Engagement Center", *In Focus* IN12475, Congress.gov, 2025, https://www.congress.gov/crs-product/IN12475. La autorización legal del GEC caducó el 23 de diciembre de 2024.

(26) CyberScoop, "State Department's Disinformation Office to Close After Funding Nixed in NDAA", *CyberScoop*, diciembre de 2024, https://cyberscoop.com/state-departments-disinformation-office-to-close-after-funding-nixed-in-ndaa/

(27) U.S. Department of Justice, National Security Division, "Foreign Agents Registration Act (FARA)", *Justice.gov*, https://www.justice.gov/nsd-fara

(28) Parlamento Europeo y Consejo de la Unión Europea, "Reglamento (UE) 2022/2065 de 19 de octubre de 2022 relativo a un mercado único de servicios digitales (Reglamento de Servicios Digitales)", *Diario Oficial de la Unión Europea* L 277, 27 de octubre de 2022, https://eur-lex.europa.eu/eli/reg/2022/2065/oj

(29) Comisión Europea, "The Code of Conduct on Disinformation", *Shaping Europe's Digital Future*, 13 de febrero de 2025, https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation. La integración del Código al marco de la Ley de Servicios Digitales surtió efecto el 1 de julio de 2025.

(30) Consejo de la Unión Europea, "Reglamento (UE) 2022/350 del Consejo de 1 de marzo de 2022", *Diario Oficial de la Unión Europea* L 65, 2 de marzo de 2022, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022R0350

(31) European Union Agency for Cybersecurity (ENISA) y European External Action Service, *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity: Threat Landscape*, ENISA, diciembre de 2022, https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape

VI. Conclusiones y recomendaciones

El caso "La Compañía", presentado siempre como operación presunta, opera como un revelador de tres conclusiones para el derecho argentino.

La primera es de orden conceptual. El jurista debe distinguir con rigor las dos acepciones del *cyber deception*, porque el engaño defensivo de redes (lícito y recomendado por los estándares técnicos) y el engaño informativo ofensivo (la amenaza) comparten un mismo núcleo, la inducción de una creencia falsa, pero ocupan posiciones jurídicas opuestas. Toda futura legislación debe cuidar de no penalizar al primero al combatir el segundo.

La segunda es de política legislativa. La respuesta argentina, de existir, debería inspirarse en un modelo de transparencia, no de censura, tomando elementos de la Ley de Registro de Agentes Extranjeros estadounidense y de la Ley de Servicios Digitales europea, obligaciones de divulgación del financiamiento extranjero de contenidos, etiquetado de medios dirigidos por Estados extranjeros y deberes de diligencia y reporte para las plataformas, sin crear delitos de "noticia falsa". Existe un umbral que invierte la recomendación: si se tipificara la desinformación como un delito de contenido, la norma colisionaría con la doctrina de la Corte Interamericana (Opinión Consultiva OC-5/85 y artículo 13 de la Convención) y sería previsiblemente inconstitucional.

La tercera es de orden práctico. En el caso concreto, el operador jurídico no debe perseguir la "desinformación" en abstracto, sino encuadrar conductas específicas en figuras existentes: el fraude informático, la suplantación de identidad mediante personas ficticias, las infracciones a la Ley de Inteligencia Nacional y, eventualmente, el lavado de activos respecto de los pagos encubiertos. El énfasis de la política pública, por lo demás, debería situarse en la "integridad informativa" (resiliencia social, alfabetización mediática, atribución pública y cooperación con organizaciones de prensa profesional como FOPEA) antes que en la restricción previa de la expresión. La amenaza por tutelar es la integridad democrática frente a la injerencia extranjera, y no la opinión política interna, cualquiera sea su signo.

VII. Bibliografía

Cariboni, Diana. "Russia Tried to Discredit Milei in Argentina, but Ended Up Damaging Its Media Instead". *openDemocracy*, mayo de 2026.

https://www.opendemocracy.net/russia-tried-to-discredit-milei-in-argentina-but-ended-up-damaging-its-media-instead/

Cariboni, Diana, Sofía Álvarez Jurado y Santiago O'Donnell. "Leña al fuego: La campaña rusa para influir en los medios de comunicación de Argentina". *openDemocracy*, 2 de abril de 2026. https://www.opendemocracy.net/es/argentina-rusia-propaganda-medios-periodismo-milei-ucrania-putin-trump-prigozhin/

Comisión Europea. "The Code of Conduct on Disinformation". *Shaping Europe's Digital Future*, 13 de febrero de 2025.

https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation

Congreso de la Nación Argentina. "Ley 25.326, Protección de los Datos Personales". Boletín Oficial, 2 de noviembre de 2000.

https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/actualizacion

Congreso de la Nación Argentina. "Ley 26.388, Código Penal. Modificación". Boletín Oficial, 25 de junio de 2008. https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto

Consejo de la Unión Europea. "Reglamento (UE) 2022/350 del Consejo de 1 de marzo de 2022". *Diario Oficial de la Unión Europea* L 65, 2 de marzo de 2022.

https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022R0350

Congressional Research Service. "Termination of the State Department's Global Engagement Center". *In Focus* IN12475. Congress.gov, 2025.

https://www.congress.gov/crs-product/IN12475

Constitución de la Nación Argentina. Boletín Oficial, 1853 (con las reformas de 1994). https://www.argentina.gob.ar/normativa/nacional/constituci%C3%B3n-de-la-naci%C3%B3n-argentina-804/texto

Corte Interamericana de Derechos Humanos. *La Colegiación Obligatoria de Periodistas (arts. 13 y 29 Convención Americana sobre Derechos Humanos)*. Opinión Consultiva OC-5/85 del 13 de noviembre de 1985. Serie A No. 5.

https://www.corteidh.or.cr/docs/opiniones/seriea_05_esp.pdf

CyberScoop. "State Department's Disinformation Office to Close After Funding Nixed in NDAA". *CyberScoop*, diciembre de 2024.

https://cyberscoop.com/state-departments-disinformation-office-to-close-after-funding-nixed-in-ndaa/

Deppe, Christoph, y Gary S. Schaal. "Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept". *Frontiers in Big Data* 7 (2024): 1452129. https://doi.org/10.3389/fdata.2024.1452129

Digital Forensic Research Lab (DFRLab) y CheckFirst. "Russia's So-Called 'Pravda' Network Expands Worldwide". *DFRLab*, 24 de febrero de 2025.

https://dfrlab.org/2025/02/24/russia-pravda-network-expands-worldwide/

European External Action Service (EEAS). "Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)". EEAS.

https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

European External Action Service (EEAS). *4th EEAS Annual Report on Foreign Information Manipulation and Interference Threats*. Bruselas, marzo de 2026.

https://www.eeas.europa.eu/eeas/4th-eeas-annual-report-foreign-information-manipulation-and-interference-threats_en

European Union Agency for Cybersecurity (ENISA) y European External Action Service. *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity: Threat Landscape*. ENISA, diciembre de 2022.

https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape

EU DisinfoLab. "Doppelganger Hub". *EU DisinfoLab*, actualizado al 7 de julio de 2025. https://www.disinfo.eu/doppelganger-hub

Forbidden Stories. "Ghost Journalists, Cash and Kremlin Scripts: How Russian Operatives Tried to Influence Argentinian Media". *Forbidden Stories*, 2 de abril de 2026.

https://forbiddenstories.org/ghost-journalists-cash-and-kremlin-scripts-how-russian-operatives-tried-to-influence-argentinian-media/

Forbidden Stories. "Propaganda Machine: Secret Documents Reveal Russia's Foreign Influence Strategy Across Three Continents". *Forbidden Stories*, abril de 2026.

https://forbiddenstories.org/propaganda-machine-secret-documents-reveal-russias-foreign-influence-strategy-across-three-continents/

Foro de Periodismo Argentino (FOPEA). "Investigación de FOPEA revela los 'mecanismos invisibles' de la desinformación extranjera en Argentina". *FOPEA*, 20 de enero de 2026.

https://fopea.org/investigacion-de-fopea-revela-los-mecanismos-invisibles-de-la-desinformacion-extranjera-en-argentina/

La Nación. "'La Compañía': documentos secretos revelan una campaña de espionaje ruso para desacreditar al gobierno de Milei". *La Nación*, abril de 2026.

https://www.lanacion.com.ar/politica/la-compania-documentos-secretos-revelan-una-campana-de-espionaje-ruso-para-desacreditar-al-gobierno-nid03042026/

Meduza. "Argentina Says It Uncovered Russian Spy Ring Suspected of Disinformation Efforts". *Meduza*, 19 de junio de 2025.

https://meduza.io/en/news/2025/06/19/argentina-says-it-uncovered-russian-spy-ring-suspected-of-disinformation-efforts

MercoPress. "Leak Reveals Russian Campaign to Discredit Milei Through Argentine Media Outlets". *MercoPress*, 4 de abril de 2026.

https://en.mercopress.com/2026/04/04/leak-reveals-russian-campaign-to-discredit-milei-through-argentine-media-outlets

NATO Allied Command Transformation. "Cognitive Warfare". *Allied Command Transformation*. https://www.act.nato.int/activities/cognitive-warfare/

National Institute of Standards and Technology (NIST). *Security and Privacy Controls for Information*

Systems and Organizations. NIST Special Publication 800-53, Revisión 5, control SC-26 (Decoys). Septiembre de 2020. https://doi.org/10.6028/NIST.SP.800-53r5

Organización de los Estados Americanos. *Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica)*. San José, 22 de noviembre de 1969.

https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm

Parlamento Europeo y Consejo de la Unión Europea. "Reglamento (UE) 2022/2065 de 19 de octubre de 2022 relativo a un mercado único de servicios digitales (Reglamento de Servicios Digitales)". *Diario Oficial de la Unión Europea* L 277, 27 de octubre de 2022. https://eur-lex.europa.eu/eli/reg/2022/2065/oj

Poder Ejecutivo Nacional (Argentina). "Decreto 941/2025, modificación de la Ley de Inteligencia Nacional y creación del Centro Nacional de Ciberseguridad". *Boletín Oficial de la República Argentina*, 2 de enero de 2026.

https://www.boletinoficial.gob.ar/detalleAviso/primera/337032/20260102

Ross, Ron, Victoria Pillitteri, Richard Graubart, Deborah Bodeau y Rosalie McQuaid. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. NIST Special Publication 800-160, Volumen 2, Revisión 1. National Institute of Standards and Technology, diciembre de 2021. https://doi.org/10.6028/NIST.SP.800-160v2r1

Spitzner, Lance. *Honeypots: Tracking Hackers*. Boston: Addison-Wesley Professional, 2002.

The MITRE Corporation. "MITRE Engage: Términos Clave (Glosario)". *MITRE Engage*, 2022. https://engage.mitre.org/learn-more-glossary/

U.S. Department of Justice. "Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere". *Office of Public Affairs*, 4 de septiembre de 2024.

https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

U.S. Department of Justice, National Security Division. "Foreign Agents Registration Act (FARA)". *Justice.gov*. https://www.justice.gov/nsd-fara

U.S. Department of State, Global Engagement Center. *GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem*. 5 de agosto de 2020.

https://2017-2021.state.gov/russias-pillars-of-disinformation-and-propaganda-report/

U.S. Department of the Treasury. "Treasury Sanctions Actors Supporting Kremlin-Directed Malign Influence Efforts". Comunicado de prensa JY2195, 20 de marzo de 2024.

https://home.treasury.gov/news/press-releases/jy2195

Zhang, Li, y Vrizlynn L. L. Thing. "Three Decades of Deception Techniques in Active Cyber Defense: Retrospect and Outlook". *Computers & Security* 106 (2021): 102288.

https://doi.org/10.1016/j.cose.2021.102288

VOCES: INTELIGENCIA ARTIFICIAL - DERECHO CONSTITUCIONAL - DERECHOS Y GARANTÍAS CONSTITUCIONALES - RESPONSABILIDAD DEL ESTADO - CONSTITUCIÓN NACIONAL - INTERNET - INFORMÁTICA - TECNOLOGÍA - PRENSA - LIBERTAD DE PRENSA - HÁBEAS DATA - PERSONA - REDES SOCIALES - DERECHOS HUMANOS - LEGITIMACIÓN PROCESAL - DERECHO DE RÉPLICA - CONTROL DE CONSTITUCIONALIDAD - DERECHO A LA INTIMIDAD - UNIÓN EUROPEA