Permanencia y actualización: El caso de NSO Group (2010-2026) como puerta de entrada de la tecnología israelí a Europa

Autora: Cèlia Carbonell Cassanyes (Irídia – Centro para la Defensa de los Derechos Humanos)

Coordinación: Alys Samson (NOVACT) y Maite Ramos (SUDS)

Comunicación: Lucrecia Baquero (Observatorio de Derechos Humanos y Empresas en el Mediterráneo)

Traducción: Lia Giralt

Maquetación: Carmela Márquez B. @edicionescaseras

Observatori de Drets Humans i Empreses · NOVACT · suds Internacionalisme Solidaritat Feminismes · Irídia · Al-Himaya Defensa de l'espai cívic a l'euromediterrània

Índice

La permanencia de NSO Group, del 2010 a la actualidad. 3

NSO Group y el gobierno Israelí: una alianza lucrativa. 5

Espiar, criminalizar y silenciar: Pegasus en Palestina. 8

Pegasus a la sombra del genocidio. 8

NSO Group en Europa, con epicentro en Luxemburgo. 10

WhatsApp vs. NSO Group y la responsabilidad de la empresa. 13

Reorientación estratégica hacia la americanización de NSO Group. 14

La permanencia de NSO Group, del 2010 a la actualidad.

A pesar del crecimiento exponencial de un gran número de empresas tecnológicas a raíz de la rápida proliferación del sector de la ciberseguridad, no se puede obviar el papel de algunas empresas israelíes, como NSO Group,[1] que revolucionaron este mercado, que en año 2010 era todavía emergente. NSO Group fue la primera empresa capaz de desarrollar una tecnología de espionaje con propiedades inéditas, como tener acceso y controlar totalmente el contenido de un dispositivo móvil a distancia y sin el permiso ni el conocimiento de la propietaria del dispositivo. Esto implica el acceso a todo el contenido del teléfono –tanto de manera retrospectiva como prospectiva–, pero también el control sobre la cámara y el micrófono.

Lejos de poder considerar Pegasus como una tecnología obsoleta, empresas como NSO Group continúan trabajando para perfeccionar y modificar las propiedades de sus productos, con el fin de lograr el objetivo inicial que dio lugar a la empresa: "desarrollar una herramienta capaz de penetrar en un dispositivo móvil de manera remota e indetectable". Niv Carmi, Shalev Hulio y Omri Lavie[2] justificaban la importancia de la tecnología que habían desarrollado señalando y apelando, desde el inicio, a una necesidad de seguridad europea: "fuerzas policiales y agencias de inteligencia de Europa nos dijeron que, con la tecnología que habíamos desarrollado, podríamos ayudar a resolver su problema".[3] Según la información publicada en su página web corporativa, la empresa "desarrolla la mejor tecnología de vigilancia para ayudar a organismos gubernamentales a detectar y prevenir el terrorismo y la delincuencia".[4] Este elemento fue el punto de partida que les llevó a fundar NSO Group Technologies Ltd. el 25 de enero de 2010.

A pesar de que NSO desarrolla un amplio abanico de productos, su producto más conocido es "Pegasus", una tecnología de vigilancia que, según la empresa, solo se vende a Estados y agencias de inteligencia a escala internacional.[5] La evolución de Pegasus ha sido constante en los últimos años: ha pasado de requerir la interacción del usuario para su activación a incorporar mecanismos de explotación de tipo cero-*click* y funcionalidades como la fabricación, modificación e inserción de información en el dispositivo.[6] Esta sofisticación progresiva acarrea consecuencias graves, puesto que el software otorga un acceso y un control total y desproporcionado sobre el contenido de los dispositivos móviles.

1 NSO Group (2010), https://www.nsogroup.com/

2 Forbidden Stories (2021). *The rise and fall of NSO Group.*

3 The New York Times (2022). *The Battle for the World's Most Powerful Cyberweapon.*

4 Más información en la página web de NSO Group, disponible en: https://www.nsogroup.com/about-us/

5 NSO Group (2025). *Transparency and Responsibility Report* 2024. 4, https://www.nsogroup.com/wp-content/uploads/2025/02/2024-Transparency-and-Responsibility-Report.pdf

6 EDRI (2025). *Spyware and state abuse: The case for an EU-wide ban.* 7—8, https://edri.org/our-work/spyware-and-state-abuse-the-case-for-an-eu-wide-ban-position-paper/

Desde el 2010 hasta la actualidad, y en particular desde el 2015, cuando se documenta por primera vez el uso de esta tecnología por parte del gobierno mexicano y, poco después, el gobierno español,[7] la empresa ha operado bajo una regulación ambigua que ha permitido una vigilancia desproporcionada y sistemática de decenas de miles de personas en todo el mundo.[8] De esta forma, se ha convertido en una herramienta creada, probada y desarrollada en un contexto de ocupación y colonialismo en Palestina, que se ofrece, se publicita y se comercializa como un instrumento de represión y persecución de la disidencia en el mundo.

Desde el inicio del genocidio en la Franja de Gaza, NSO Group ha seguido apareciendo de manera recurrente en los medios, con el objetivo de impulsar una estrategia de lavado reputacional, tras años de escándalos y denuncias públicas. En el Estado español se han acumulado una decena de querellas por el espionaje ilegal con Pegasus desde que, en abril de 2022, un informe de The Citizen Lab[9] corroboró el peligro planteado por una notificación de WhatsApp a 1.400 personas usuarias,[10] entre las que estaban el ex presidente del Parlamento de Cataluña, Roger Torrent, y el ex diputado de #ERC, Ernest Maragall, quienes se querellaron contra el #CNI y NSO Group por el uso de Pegasus el 2020.[11]

El informe de The Citizen Lab, confirmado por el laboratorio forense de Amnistía Internacional, identificaba al menos a 65 personas relacionadas con el movimiento independentista y por la autodeterminación de Cataluña como objetivos del espionaje con Pegasus y Candiru; entre ellas, abogadas, periodistas, defensoras de derechos humanos y representantes políticas en el Parlamento de Cataluña y en el Parlamento Europeo. Uno de estos casos se ha convertido en la primera denuncia de una persona afectada con Pegasus que ha conseguido la imputación de tres cargos directivos de la empresa NSO Group en Israel y Luxemburgo,[12] entre ellos dos de sus fundadores, Shalev Hulio y Omri Lavie, que se encuentran actualmente investigados en una causa penal en un juzgado de Barcelona.

7 El Diario.es (2025). *Artur Mas fue el primer espiado con Pegasus en España cuando era presidente en 2015, según Citizen Lab*, https://www.eldiario.es/catalunya/artur-primer-espiado-pegasus-espana-president-citizen-lab_1_12270015.html

8 Forbidden Stories (2021). *About the Pegasus Projec*t, https://forbiddenstories.org/about-the-pegasus-project/

9 The Citizen Lab (2022). *CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru,* https://citizenlab.ca/research/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

10 Tech Crunch (2019). *WhatsApp blames —and sues— mobile spyware maker NSO Group over its zero-day calling exploit*, https://techcrunch.com/2019/10/29/whatsapp-spyware-nso-group/

11 El Diario.es (2020). *Torrent se querella contra el exdirector del CNI por "espionaje político" y pide al juez comprobar si el Gobierno contrató el programa Pegasus*, https://www.eldiario.es/catalunya/torrent-querella-exdirector-cni-espionaje-politico-pide-juez-comprobar-si-gobierno-contrato-programa-pegasus_1_6136003.html

12 Irídia — Centre per la defensa dels drets humans (2025). *Tres directius de NSO Group imputats per la seva responsabilitat en l'espionatge amb Pegasus*, https://iridia.cat/tres-directius-de-nso-group-imputats-per-la-seva-responsabilitat-en-lespionatge-amb-pegasus/

Desde sus inicios, NSO Group ha destacado que su tecnología tiene origen directo en la experiencia militar israelí. Como demuestra el informe "Las puertas de entrada de la tecnología del genocidio a Europa", es habitual que los fundadores de empresas de este sector provengan de unidades de inteligencia del ejército israelí, como por ejemplo la Unidad 8200, la Unidad 81 o el Mossad.[13] En este caso, el creador técnico de NSO Group, Niv Carmi (la N de NSO), había sido agente de inteligencia y experto en seguridad del Mosaad. Un caso reciente, del mismo sector de mercado y que responde a la misma lógica es el caso de Paragon Solutions,[14] fundada a Israel el 2019 por Ehud Barak, exministro israelí, y Ehud Schneorson, excomandante de la Unidad 8200. El producto principal de esta empresa es Graphite,[15] un software espía con capacidades técnicas[16] equiparables a las de Pegasus, protagonista del último escándalo con software espía en Italia.[17]

Tal como decreta la ley israelí en materia de exportación de "productos de defensa", la Agencia de Control de Exportación de Defensa (DECA), competencia del Ministerio de Defensa de Israel, es la autoridad encargada de la exportación de licencias de empresas como NSO Group,[18] siendo el único ente responsable de supervisar y controlar la comercialización de esta tecnología con fines lucrativas a escala mundial. Si bien esta autorización es el argumento que suele esgrimir la empresa para justificar la existencia de un supuesto mecanismo de control externo, a la vez, evidencia su relación directa con el gobierno de Israel.

NSO Group y el gobierno Israelí: una alianza lucrativa.

Tras 15 años de actividad, numerosos artículos y estudios demuestran como NSO Group se ha convertido en un símbolo de la industria cibernética ofensiva de Israel, públicamente publicitada como una herramienta de exportación estratégica al servicio del gobierno. Comercializado bajo el sello de "alta tecnología de defensa hecha en Israel", Pegasus se

13 Forbidden Stories (2021). *The rise and fall of NSO Group*, https://forbiddenstories.org/the-rise-and-fall-of-nso-group/

14 The Citizen Lab (2025). *Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations,* https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/

15 The Citizen Lab (2025). *Graphite Caught. First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted*, https://citizenlab.ca/2025/06/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/

16 Amnesty International (2025). *Italy: New case of journalist targeted with Graphite spyware confirms widespread use of unlawful surveillance*, https://www.amnesty.org/en/latest/news/2025/06/italy-new-case-of-journalist-targeted-with-graphite-spyware-confirms-widespread-use-of-unlawful-surveillance/

17 The Guardian (2026). I*talian activists and journalist targeted by spyware in 2024, prosecutors confirm,* https://www.theguardian.com/world/2026/mar/06/italy-activists-and-journalist-targeted-by-spyware-in-2024-prosecutors-confirm

18 NSO Group (2024), *Transparency and Responsibility Report 2024*, https://www.nsogroup.com/wp-content/uploads/2025/02/2024-Transparency-and-Responsibility-Report.pdf

ha promovido como un instrumento central de la política exterior israelí para reforzar, ampliar y consolidar relaciones diplomáticas. Esta actividad ha ido acompañada de una campaña de legitimación pública, articulada alrededor de cuatro ejes —securitització, normalización, limpieza ética (*ethics washing*) y el patriotismo sionista—[19] que presentan la vigilancia como la única respuesta viable a los retos de seguridad.[20] Este es un argumento recurrente, utilizado también en el proceso de desregulación y simplificación europeo, para justificar no únicamente el uso de estas herramientas, sino su misma existencia, normalizándola como algo inevitable en nombre de la innovación.

Esta dinámica ha generado un intercambio claro: beneficios económicos para la empresa y capacidad de influencia geopolítica para Israel. Varias investigaciones han demostrado una correlación directa entre visitas o reuniones de jefes de estado con representantes del gobierno israelí y la autorización de nuevas licencias de exportación de Pegasus. Este patrón se ha repetido tanto en procesos de normalización diplomática, como moneda de intercambio para mejorar las relaciones diplomáticas con el gobierno de Israel (como en los casos de Hungría, Polonia, Ruanda, Azerbaiyán o India),[21] como en negociaciones políticas internacionales, incluyendo votaciones en las Naciones Unidas, como en el caso de México y Panamá.[22]

En el caso de Panamá, una investigación conjunta del Organized Crime and Corruption Reporting Project (OCCRP) —socio de *Forbidden Stories*—, *Código Morse y Shomrim*[23] ha aportado un nuevo elemento que pone de manifiesto esta relación de dependencia entre la empresa y el Gobierno de Israel. Según la investigación, publicada el 16 de julio de 2026, Shalev Hulio, uno de los fundadores de NSO Group, habría utilizado un pasaporte diplomático israelí para entrar en Panamá el 3 de diciembre de 2013. De acuerdo con los registros migratorios panameños, Hulio habría entrado en el país como "diplomático" en una visita que él mismo calificó de "recreativa", y habría declarado a las autoridades de inmigración que se alojaría en la embajada de Israel. Un año antes, en 2012, el Gobierno de Panamá habría firmado un contrato con NSO en un proceso liderado por el propio Hulio.

19 Kotliar, D. M., & Carmi, E. (2023). *Keeping Pegasus on the wing: legitimizing cyber espionage. Information, Communication & Society, 27(8)*, 1499–1529. https://doi.org/10.1080/1369118X.2023.2245873

20 Ibid. 1500–1501.

21 Haaretz (2021). *The Pegasus Project: Where Netanyahu Went, NSO Followed: How Israel Pushed Cyberweapon Sales,* https://www.haaretz.com/israel-news/tech-news/2021-07-20/ty-article/.highlight/where-bibi-went-nso-followed-how-israel-pushed-cyberweapons-sales/0000017f-e388-d7b2-a77f-e38fd45a0000

22 The New York Times (2022). *The Battle for the World's Most Powerful Cyberweapon, A Times investigation reveals how Israel reaped diplomatic gains around the world from NSO's Pegasus spyware — a tool America itself purchased but is now trying to ban,* https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html

23 OCCRP (2026). Cofundador de controvertida empresa de software espía tenía pasaporte diplomático israelí, https://www.occrp.org/es/investigacion/co-founder-of-controversial-spyware-firm-had-israeli-diplomatic-passport

El exdirectivo de NSO ha negado estas informaciones, pero varias personas expertas consideran que la investigación vuelve a poner el foco en la posible relación entre ambos actores. El abogado israelí Eitay Mack, conocido por su larga trayectoria contra el uso de Pegasus, lo resume así: "[Pegasus] es una herramienta importante para que Israel construya vínculos, especialmente con las unidades de inteligencia de países extranjeros [...]. Es una de sus principales herramientas para crear y mantener relaciones exteriores".[24]

En los últimos años, la exportación y la comercialización de Pegasus también ha jugado un papel destacado en la normalización de las relaciones de Israel con varios países del Golfo[25] y en el marco de los Acuerdos de Abraham de 2020,[26] con el objetivo de asegurar el apoyo diplomático de las naciones árabes a Israel. El grado de influencia del gobierno israelí sobre la empresa es tal que, incluso después de que NSO Group rompiese el contrato de Pegasus con Arabia Saudí por la presunta implicación en el asesinato del columnista del Washington Post Jamal Khashoggi en consulado saudí de Estambul en el 2018, la autorización fue restablecida[27] al tras una llamada entre el príncipe heredero Mohammed bin Salman y Benjamin Netanyahu.

El poder de influencia de Pegasus se puso también en evidencia a raíz de una publicación del embajador israelí en funciones en la red social X, en la que amenazaba al gobierno de Pedro Sánchez con utilizar y publicar toda la información relativa al caso Pegasus en el Estado español[28]. Algunos medios de comunicación documentaron la publicación para que quedara constancia, a pesar de que fue borrada.[29] Esta publicación se hizo horas después de que el presidente español reconociera el estado palestino.

24 Ibid.

25 Haaretz (2022). *NSO Played Key Role in Israel's Gulf Diplomacy, NYT Finds, Confirming Haaretz Reports*, https://www.haaretz.com/israel-news/2022-01-28/ty-article/.premium/netanyahu-gave-greenlight-to-saudi-arabia-to-use-nso-spyware-report-says/0000017f-dc3d-d3ff-a7ff-fdbd5a680000

26 Los Acuerdos de Abraham son un conjunto de acuerdos bilaterales impulsados por los Estados Unidos durante la primera administración Trump, con el objetivo de normalizar las relaciones diplomáticas entre Israel y varios países árabes. El primer acuerdo se firmó el 15 de septiembre de 2020 entre Israel, los Emiratos Árabes Unidos y Baréin. Posteriormente, se añadieron Sudán (octubre de 2020) y Marruecos (diciembre de 2020). Estos acuerdos representan la primera normalización formal de las relaciones árabes-israelíes desde el tratado de paz entre Israel y Jordania de 1994 y el acuerdo entre Egipto e israel de 1979.

27 The New York Times (2021), I*sraeli Companies Aided Saudi Spying Despite Khashoggi Killing*, https://www.nytimes.com/2021/07/17/world/middleeast/israel-saudi-khashoggi-hacking-nso.html

28 El uso de Pegasus en el Estado español se ha identificado a través de dos casos diferentes. El primer caso es el que se recoge en este informe, referente al Catalan Gat; el segundo afecta a representantes políticos del actual gobierno español, caso en el que se señala a Marruecos como presunto autor del espionaje.

29 Diario Red (2025). *El embajador de Israel en funciones amenaza al Gobierno de España con revelar información obtenida con 'Pegasus'*, https://www.diario-red.com/articulo/espana/embajador-israel-funciones-amenaza-gobierno-espana-revelar-informacion-obtenida-pegasus/20250529191025048336.html

Espiar, criminalizar y silenciar: Pegasus en Palestina.

A pesar de que Pegasus es el caso más conocido, solo es la punta del iceberg en la exportación de tecnología de ciber vigilancia israelí utilizada para el control autoritario en todo el mundo. A menudo se olvida que estos sistemas se han diseñado y probado en el contexto del régimen de ocupación, colonialismo y apartheid en Palestina, y que también se han empleado para sabotear y criminalizar organizaciones palestinas de derechos humanos. El noviembre de 2021, poco después de que seis organizaciones palestinas de derechos humanos fueran calificadas por Israel como "terroristas", [30] se descubrió que seis personas que trabajaban en dichas organizaciones habían sido espiadas con Pegasus. [31]

El espionaje contribuye al ciclo de criminalización y pretende silenciar entidades como Al-Haq, Addameer o el Bisan Center, que desde hace años documentan y denuncian los crímenes de guerra y de lesa humanidad cometidos por Israel contra el pueblo palestino. Las consecuencias para las personas palestinas afectadas van mucho más allá de la simple ilegalización de su trabajo. En el caso del defensor de los derechos humanos Salah Hamouri,[32] fue encarcelado y posteriormente deportado a Francia,[33] sin posibilidad de volver a Palestina ni de continuar ejerciendo su tarea como abogado en los tribunales militares israelíes.

Pegasus a la sombra del genocidio.

La vinculación con determinados núcleos militares y de inteligencia de Israel forma parte de una estrategia de estado orientada a proyectar prestigio y a reforzar la percepción de calidad tecnológica de los productos ofrecidos. Esta estrategia comunicativa se ha visto especialmente acentuada desde el inicio del genocidio en la Franja de Gaza, momento en que las empresas tecnológicas vinculadas al complejo militar israelí han reforzado el discurso que asocia su experiencia en contextos de "seguridad nacional" con la eficacia y la fiabilidad de sus productos. Esta ha sido la tesis principal de NSO Group para intentar reintroducirse en el mercado norteamericano tras haber sido incluida en la denominada

30 United Nations Human Rights Office of the High Commissioner (OHCHR) (2021). UN experts condemn Israel's designation of Palestinian human rights defenders as terrorist organisations, https://www.ohchr.org/en/press-releases/2021/10/un-experts-condemn-israels-designation-palestinian-human-rights-defenders

31 Amnesty International (2021). *Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware*, https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/

32 Addameer (2022). *Lawsuit filed against Israeli spyware company NSO*, https://addameer.ps/es/news/4743

33 Front Line Defenders (2022). *Detained human rights defender Salah Hammouri was forcibly deported to France*, https://www.frontlinedefenders.org/en/case/detained-human-rights-defender-salah-hammouri-was-forcibly-deported-france

lista de sanciones del Departamento de Comercio de los Estados Unidos,[34] el 3 de noviembre de 2021, bajo la justificación de "situar los derechos humanos en el centro de la política exterior de Estados Unidos".[35]

Desde octubre de 2023, NSO Group, junto con una larga lista empresas israelíes de ciberseguridad, se ofreció voluntariamente para colaborar en la misión de localizar los rehenes israelíes.[36] De facto, NSO Group inició un proceso de actualización de su tecnología militar de vigilancia, con el objetivo de atender esta necesidad. A pesar de la alta competencia del mercado, desde el 7 de octubre estas empresas estarían colaborando en un esfuerzo conjunto sin precedentes, para apoyar en un frente común de "inteligencia" digital, que ha reforzado la promoción de la tecnología israelí como única en el mundo. Organizaciones internacionales como Democracy for the Arab World Now (DAWN) han descrito estos movimientos como "un intento de la empresa de restablecer su imagen en plena crisis".[37]

A partir de octubre de 2023, queda claro que, en un despliegue bélico sin precedentes, el gobierno israelí vuelve a permitir que NSO asuma un papel relevante y destacado. En un pódcast del medio de comunicación israelí Haaretz, publicado el 19 de octubre de 2023[38] —formato que, según varios analistas, está sujeto a menos censura que la prensa escrita en Israel—, se analiza como NSO se pone al servicio del gobierno, asumiendo tareas significativas para el Ministerio de Defensa. Este hecho, lejos de ser excepcional o novedoso, pone de manifiesto la continuidad de la colaboración histórica entre la empresa y el gobierno de Israel. Todo esto fue acompañado del anuncio, en enero de 2024,[39] del traslado de la sede de NSO Group a unas oficinas más grandes, como parte de un plan de expansión corporativa.

Actualmente, no se sabe con certeza hasta qué punto ni de qué manera se está utilizando Pegasus en la Franja de Gaza. El que sí que está claro es que las fuerzas de ocupación israelíes despliegan todo su arsenal tecnológico, tal y como reafirma este informe. Medios de investigación como la revista +972 Magazine[40] han alertado sobre una herramienta

34 The Intercept (2023). *Israeli Spyware Firm NSO Demands "Urgent" Meeting With Blinken Amid Gaza War Lobbying Effort*, https://theintercept.com/2023/11/10/nso-group-israel-gaza-blacklist/

35 Ibid.

36 Haaretz (2023). *NSO, Israeli Cyber Firms Help Track Missing Israelis and Hostages*, https://www.haaretz.com/israel-news/security-aviation/2023-10-19/ty-article/.premium/israeli-cyber-arms-and-intelligence-firms-like-nso-aiding-israeli-efforts/0000018b-4813-de3d-a58f-c87b7d950000?v=1698415601171

37 The Intercept (2023). I*sraeli Spyware Firm NSO Demands "Urgent" Meeting With Blinken Amid Gaza War Lobbying Effort.*

38 Haaretz (2023). *יאיר גולן: השיח של ההרתעה הוא פרימיטיבי. הפעילות מול חמאס תימשך שנים* , https://www.haaretz.co.il/digital/podcast/weekly/2023-10-19/ty-article-podcast/0000018b-470f-df22-a5eb-4f7fb1be0000

39 Globes (2024). *Israeli spyware co NSO moving to bigger offices*, https://en.globes.co.il/en/article-israeli-spyware-co-nso-moving-to-bigger-offices-1001466834

40 +972 Magazine (2024). *'Lavender': The AI machine directing Israel's bombing spree in Gaza*, https://www.972mag.com/lavender-ai-israeli-army-gaza/

específica basada en inteligencia artificial destinada a elaborar listas de posibles "objetivos" militares. Este sistema analiza y cruza grandes volúmenes de datos con mucha rapidez e identifica miles de personas o lugares, como por ejemplo viviendas, para bombardearlos. En el caso de Lavender —descrito como la máquina de inteligencia artificial que dirige los bombardeos de Israel en la Franja de Gaza—,[41] la verificación incluye la ubicación de los teléfonos o grabaciones de voz para determinar si la persona es hombre o mujer; siente el único procedimiento que permite al sistema confirmar que el dispositivo corresponde a la persona señalada. Dado que Pegasus permite acceder y controlar a distancia un dispositivo móvil, incluyendo la geolocalización y la activación del micrófono, algunos expertos internacionales han señalado que las capacidades de este software han tenido un papel crítico y fundamental en la obtención de datos a la Franja de Gaza durante el genocidio en curso,[42] en el marco de lo que se ha descrito como una "fábrica de asesinatos en masa".[43]

NSO Group en Europa, con epicentro en Luxemburgo.

Si bien la empresa justifica su producto por razones de "seguridad nacional", los datos disponibles muestran centenares de miles de casos en los que esta tecnología se ha utilizado contra actores de la sociedad civil[44] que no representaban ninguna amenaza para los estados implicados. Estas prácticas fomentan la construcción de un "futurible delictivo", es decir, la presunta existencia de una amenaza sin fundamento, un mecanismo habitual en el uso de tecnologías de vigilancia. Ante esta situación, numeroses organizaciones internacionales han pedido la prohibición de Pegasus.[45]

A pesar de que NSO Group Technologies Ltd. es una empresa privada incorporada y registrada en Israel, el nombre "NSO Group" se utiliza como marca paraguas para designar el conjunto de empresas asociadas, tanto operativas como financieras, distribuidas por todo el mundo. La estructura corporativa de NSO[46] refleja la rápida expansión y proliferación de

41 La Directa (2024). *Lavender: la màquina d'intel·ligència artificial que dirigeix el bombardeig d'Israel a Gaza*, https://directa.cat/lavender-la-maquina-dintelligencia-artificial-que-dirigeix-el-bombardeig-disrael-a-gaza/

42 Youtube (2024). *Roda de premsa Irídia vs. Pegasus. Minut* 35:57—38:30, https://www.youtube.com/watch?v=l3zqiwFJtyA&t=1s

43 +972 Magazine (2023). *'A mass assassination factory': Inside Israel's calculated bombing of Gaza*, https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/

44 Forbidden Stories (2021). *The Pegasus Project, Global Democracy under cyber attack*, https://forbiddenstories.org/about-the-pegasus-project/

45 EDRI (2025). S*pyware and state abuse: The case for an EU-wide ban*.

46 La marca comercial "NSO Group" es propiedad exclusiva de la empresa matriz israelí NSO Group Technologies Ltd.

este sector, y advierte de una realidad preocupante en la actualidad.[47] Con un total de 13 sociedades holding y 12 filiales en múltiples jurisdicciones, el grupo opera mediante una estructura dendrítica y deliberadamente opaca, en la que las empresas a menudo cambian estratégicamente de nombre y amplían sus actividades a otras jurisdicciones para eludir regulaciones más estrictas.[48] Es por eso que resulta fundamental analizar como se introduce y actúa en Europa como un espejo de prácticas y lógicas que se reproducen dentro del mercado de la vigilancia. Un elemento estructural de este tipo de empresas es la carencia de transparencia y de mecanismos efectivos de rendición de cuentas sobre sus actividades y exportaciones, hecho que dificulta el acceso a información verificable, incluidas las causas judiciales iniciadas por personas espiadas con Pegasus.[49]

El entramado empresarial de NSO cuenta con una presencia especialmente significativa en Luxemburgo. Luxemburgo, miembro fundador de la UE y de la zona euro, se ha consolidado como un hub estratégico para empresas internacionales, gracias al acceso al mercado europeo, un marco empresarial flexible, infraestructuras tecnológicas avanzadas, estabilidad económica y una especialización destacada en ciberseguridad. Además Israel lo promueve activamente como destino para la expansión empresarial.[50] En el momento de redacción de este informe, NSO tiene diecinueve sociedades domiciliadas, once de las cuales comparten el mismo objeto social.[51] Esta estructura corporativa amplía el abanico de actuación de estas entidades, otorgándoles un carácter instrumental, puesto que amplía su ámbito de actuación sin definir con claridad la finalidad. Además, las sociedades comparten no solo el objeto social sino también la ubicación física.[52]

El informe final de la Comisión PEGA del Parlamento Europeo,[53] concluyó que el mantenimiento de NSO depende en gran medida del apoyo de las sociedades establecidas en Luxemburgo. El informe identificaba estas entidades como el centro de negocios europeo del grupo, que facilita su actividad con una regulación menos estricta tanto dentro de la UE como en terceros países, y gestiona facturación, contratos y pagos vin-

47 EDRI (2025). *Spyware and state abuse: The case for an EU-wide ban*.

48 SMEX (2025). *Click, Load, Kill: A Look into the Cyberweapon industry in the WANA Region*. 28—45, https://smex.org/new-research-click-load-kill-a-look-into-the-cyberweapon-industry-in-the-wana-region/

49 El Diario.es (2025). *La exjefa del CNI vuelve a escudarse en que la ley le impide declarar por el espionaje a dos diputados de ERC*, https://www.eldiario.es/catalunya/exjefa-cni-vuelve-escudarse-ley-le-impide-declarar-espionaje-diputados-erc_1_12640307.html

50 Luxembourg Trade & Invest. *Your gateway to Luxembourg and Israel*, https://luxembourgtradeandinvest.com/our-international-network/ltio-tel-aviv

51 El objeto social de once de estas sociedades es ser designadas formalmente, mediante contrato, acuerdo social o decisión de un órgano competente, para ejercer cargos o funciones en otras sociedades, y actuar como socias directoras generales, adquirir participaciones en Luxemburgo o en extranjero e intervenir en su gestión.

52 De las diecinueve sociedades de NSO Group en Luxemburgo, catorce tienen el mismo domicilio social, mientras que las cinco restantes se encuentran concentradas en otra dirección.

53 Durante un año investigó los casos de espionajes con Pegasus en la Unión Europea con especial atención en Hungría, Polonia, Grecia y el Estado español. Más información en: https://www.europarl.europa.eu/regdata/etudes/brie/2024/761472/ipol_bri(2024)761472_EN.pdf

culados al software espía.[54] La permisividad de la UE hacia el mercado de software espía comercial no solo favorece que estas empresas operen bajo un marco normativo más laxo, sino que también dota de legitimidad la comercialización de sus productos desde territorio europeo.

Entre las diecinueve sociedades vinculadas a NSO Group registradas en Luxemburgo, destacan Osy Technologies Sàrl y Q Cyber Technologies Sàrl, tanto por su vínculo con la cibertecnologia como por su relevancia estructural dentro del grupo. Osy Technologies, creada en febrero de 2014, fue la primera sociedad del grupo en el país, seguida de Q Cyber Technologies, constituida en enero de 2016 con Osy como accionista único. Ambas se sitúan en el núcleo originario de la presencia europea del grupo, que se consolidó posteriormente mediante una rápida expansión societaria —tres el 2017, cuatro el 2018 y cinco el 2020. Osy y Q Cyber mantienen lazos directos con NSO Group Technologies, hasta el punto de compartir junta directiva en los primeros años. Dos de los fundadores de NSO, Omri Lavie y Shalev Hulio, tienen una presencia destacada.[55]

Según la justicia israelí, esta estructura también tendría una finalidad fiscal. En agosto de 2026, un tribunal israelí condenó a NSO Group por fraude. Según la sentencia, entre 2014 y 2018 el grupo recibió 86 millones de dólares en beneficios a través de Osy sin pagar los impuestos correspondientes en Israel.[56] El tribunal también concluyó que la estructura de propiedad de NSO a través de Osy se creó, al menos en parte, para reducir los impuestos de sus operaciones de endeudamiento y financiación.

Además del objetivo fiscal, la presencia en Luxemburgo también ha servido para construir una nueva imagen.

Es preciso destacar que, cuando el 14 de febrero de 2019 el equipo directivo y fundador de NSO Group anunció que la firma de capital privado británica Novalpina Capital asumía el control, el grupo ya se presentaba como una "empresa de tecnología cibernética con sede en Luxemburgo", resultado de la "fusión de empresas de tecnología cibernética israelíes y europeas".[57] Esta presentación no pretendía únicamente reformular la identidad corporativa del grupo bajo una apariencia más europea, sino que también respondía a una estrategia de posicionamiento institucional orientada a legitimar su actividad dentro del mercado europeo de la ciberseguridad y pretendía distanciarse parcialmente de su

54 European Parliament (2023). *REPORT of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware*. 397—399, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html

55 Lavie aparece en nueve juntas directivas de sociedades luxemburguesas y Hulio en seis, reforzando la idea de una estructura interconectada y gestionada de manera unificada.

56 Lexology (2026). Q Cyber Technologies Ruling: District Court Holds That a Leveraged Acquisition Structure May Constitute an Artificial Transaction, https://www.lexology.com/library/detail.aspx?g=4c2105a1-094c-410e-a495-7d50ac920f64

57 Amnesty International, Privacy International & SOMO (2021). *Operating from the Shadows: Inside NSO Group's Corporate Structure*. 42—27, https://www.amnesty.org/es/documents/doc10/4182/2021/en/

vinculación directa con Israel, especialmente a raíz de las controversias generadas por el uso de Pegasus. No obstante, esta línea identitaria más difusa, que permite un acceso más permeable al mercado mundial, choca con los valores fundacionales del grupo, reafirmados después de octubre de 2023, cuando el grupo cerró filas con el gobierno israelí.

A raíz de los escándalos de Pegasus, a mediados de 2022, Shalev Hulio dimitió como CEO de NSO Group y fue sustituído por Yaron Shohat. En enero de 2023, Hulio fundó Dream Security.[58] El 7 de noviembre de 2023, desde la Franja de Gaza, desde donde servía como reservista israelí, Hulio anunció una ronda de financiación,[59] que presentó como un "gran mensaje para la comunidad tecnológica y para el pueblo de Israel".[60] A pesar de sus intentos por desvincularse de NSO Group, una docena de antiguos altos cargos y operativos lo han seguido a Dream Security, donde la mayoría del personal está en Israel a pesar de que disponen de oficinas en Tel Aviv, Viena y Abu Dabi. La empresa ha nacido rodeada de controversia por sus vínculos con la derecha israelí e internacional, especialmente por la participación como cofundador del excanciller austríaco Sebastian Kurz.[61] En su rápida expansión, Dream Security sigue la estela de NSO Group, manteniendo una presencia destacada a Europa.

WhatsApp vs. NSO Group y la responsabilidad de la empresa.

La denuncia presentada por WhatsApp y Meta contra NSO Group el 2019 en Estados Unidos[62] marcó un punto de inflexión en la crisis reputacional de la empresa. Durante el proceso, el Departamento de Comercio norteamericano incluyó NSO Group en su lista de sanciones el 2021,[63] al considerar que sus actividades contravenían los intereses de seguridad nacional. Desde entonces, NSO Group tiene prohibido operar en el mercado estadounidense y su personal tiene restringido el acceso al país.[64] A pesar del impacto econó-

58 Dream Security es una start-up dedicada a soluciones defensivas de ciberseguridad para infraestructuras críticas, con la ambición pública de convertirse en la "mejor plataforma defensiva de ciberseguridad basada en inteligencia artificial del mundo". Más información disponible en: https://dreamgroup.com/about/

59 The Intercept (2024). *In Video From Gaza, Former CEO of Pegasus Spyware Firm Announces Millions for New Venture,* https://theintercept.com/2024/01/18/israel-nso-group-shalev-hulio-dream-security/

60 El Salto Diario (2024). *Los señores israelíes de la ciberguerra,* https://www.elsaltodiario.com/espionaje/senores-israelies-ciberguerra-pegasus-predator

61 Follow The Money (2025). *The Talented Mr. Kurz: How Austria's Ex-Leader Leader made it big in Israeli Cyber industry*, https://www.ftm.eu/articles/spyware-sebastian-kurz

62 The New York Times (2019). *WhatsApp Says Israeli Firm Used Its App in Spy Program*, https://www.nytimes.com/2019/10/29/technology/whatsapp-nso-lawsuit.html?auth=login-email&login=email

63 The Guardian (2021). Israeli spyware company NSO Group placed on US blacklist, https://www.theguardian.com/us-news/2021/nov/03/nso-group-pegasus-spyware-us-blacklist

64 The Guardian (2024). *US announces new restrictions to curb global spyware industry*, https://www.theguardian.com/us-news/2024/feb/05/us-biden-administration-global-spyware-restrictions

mico y político de esta sanción, la Unión Europea no ha adoptado medidas equivalentes ni ha establecido una posición común sobre la prohibición de Pegasus.

El diciembre de 2024, un tribunal de California condenó NSO Group por vulnerar leyes federales y estatales de fraude y abuso informático y falló a favor de WhatsApp,[65] imponiendo una indemnización superior a los 168 millones de dólares.[66] El procedimiento también volvió a posar de manifiesto la opacidad del grupo y demostró que es NSO Group quién realiza las fases iniciales de infección y extracción de datos de los dispositivos atacados, contrariando el relato que había sostenido hasta ahora.[67] La sentencia ha sido celebrada internacionalmente como un hito clave en la lucha contra los abusos de los programas espía.[68]

Reorientación estratégica hacia la americanización de NSO Group.

Aunque la crisis reputacional de NSO Group obligó a reubicar a decenas de trabajadoras, la empresa continuó operando hasta noviembre de 2025 bajo el liderazgo de uno de sus fundadores, Omri Lavie. Tras 25 años de actividad y con más de 22 clientes solo en Europa (incluyendo 12 de los 27 estados miembro),[69] en noviembre de 2025 se produjo un cambio sustancial en la dirección. Por primera vez, los fundadores —algunos activos desde 2010— dejaron de tener cualquier participación, hecho que marca un punto de inflexión en la trayectoria de la empresa.

La nueva etapa, encabezada por el abogado norteamericano David Friedman,[70] coincide con la adquisición total de la compañía por parte de un grupo de inversores de los Estados Unidos (algunos con nacionalidad israelí), lo que pone de manifiesto su conexión con el

65 Sentencia procedimiento WhatsApp v. NSO Group (2024). Para mayor información consulta: https://www.documentcloud.org/documents/25467209-gov/

66 The Record Media (2025). *Jury orders NSO Group to pay $168 million to WhatsApp for facilitating Pegasus hacks of its users*, https://therecord.media/jury-orders-nso-to-pay-meta-168-million-over-whatsapp-hack

67 The Guardian (2024). *NSO – not government clients – operates its spyware, legal documents reveal*, https://www.theguardian.com/technology/2024/nov/14/nso-pegasus-spyware-whatsapp

68 Access Now (2025). *Statement on the historic decision in the WhatsApp v NSO case*, https://www.accessnow.org/press-release/statement-on-whatsapp-v-nso-case-decision/

69 Haaretz (2022), Pegasus Spyware Maker NSO Has 22 Clients in the European Union. And It's Not Alone, https://www.haaretz.com/israel-news/security-aviation/2022-08-09/ty-article/.premium/israeli-spyware-maker-nso-has-22-customers-in-12-eu-countries-and-its-not-alone/00000182-8403-df1d-a3a7-ae9bce800000

70 Haaretz (2025), *Ex-Trump Ambassador to Israel David Friedman Named NSO Chairman, as Spyware Firm Shifts to U.S. Ownership*, https://www.haaretz.com/israel-news/security-aviation/2025-11-09/ty-article/.premium/ex-trump-ambassador-to-israel-named-nso-chairman-as-spyware-firm-shifts-to-u-s-ownership/0000019a-68f4-da41-a9fe-79f7966f0000

gobierno israelí y con sectores de la extrema derecha. El actual presidente ejecutivo fue el embajador de los EE. UU. en Israel durante la primera administración Trump y participó en la negociación de los Acuerdos de Abraham. También destaca por sus intervenciones públicas en defensa de los asentamientos ilegales en el Territorio Palestino Ocupado y por impulsar campañas de financiación destinadas a este objetivo. Este cambio en la dirección y la propiedad se enmarca en una tendencia de americanización de NSO Group.

Este cambio marca un nuevo rumbo para el grupo empresarial: sobre el papel, ahora es una empresa estadounidense, pero sigue operando de manera efectiva desde Israel. Es también el caso de Paragon, que en diciembre de 2024 se fusionó con REDLattice,[71] una empresa estadounidense de ciberseguridad ofensiva propiedad del fondo AE Industrial Partners. Y también el de Candiru, adquirida por la firma de inversión estadounidense Integrity Partners.[72] Ahora, las tres empresas compiten por obtener contratos en Estados Unidos, a pesar de las sanciones impuestas.

En el contexto actual, un número creciente de empresas israelíes está optando por trasladarse o abrir filiales en Europa (una práctica ya presente desde hace años, pero actualmente intensificada), atraídas por un entorno legislativo más permisivo que facilita la proliferación y la expansión del mercado europeo de software espía comercial.[73]

Paralelamente, el cambio de dirección y de propiedad ha comportado modificaciones en tres sociedades de NSO Group registradas en Luxemburgo,[74] que pasan a estar dirigidas por Ohad Shazar Shalem Schremer.75 El abogado israelí reside al asentamiento ilegal de Neve Daniel, en Gush Etzion, dentro del Territorio Palestino Ocupado, y forma parte de la junta directiva de una asociación de colonos. Este nuevo liderazgo refleja una orientación corporativa alineada con la extrema derecha, tanto en Israel como escala internacional, y con intereses de carácter colonial.

71 Wired (2026). The Secrets of a US Spyware King, https://www.wired.com/story/the-secrets-of-the-us-spyware-king/

72 Ibid.

73 Para más información, ir al apartado IV.2 (página 37) sobre el marco regulatorio a Europa.

74 Las tres sociedades de NSO Group en Luxemburgo que cambian de dirección son: NorthPole Newco, Osy Technologies y Q Cyber Technologies.

75 Ibid.