Permanència i actualització: El cas de NSO Group (2010-2026) com a porta d'entrada de la tecnologia israeliana a Europa

Autora: Cèlia Carbonell Cassanyes (Irídia – Centre per la Defensa dels Drets Humans)

Coordinació: Alys Samson (NOVACT) i Maite Ramos (SUDS)

Comunicació: Lucrecia Baquero (Observatori de Drets Humans i Empreses a la Mediterrània)

Traducció: Lia Giralt

Maquetació: 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

Index

La permanència de NSO Group
de 2010 a l'actualitat. 3

NSO Group i el govern israelià:
una aliança lucrativa. 5

Espiar, criminalitzar i silenciar:
Pegasus a Palestina. 7

Pegasus a l'ombra del genocidi. 8

NSO Group a Europa,
amb epicentre a Luxemburg. 10

WhatsApp vs. NSO Group i la
responsabilitat de l'empresa. 13

Reorientació estratègica cap
a l'americanització de NSO Group. 14

La permanència de NSO Group de 2010 a l'actualitat.

Malgrat el creixement exponencial d'un gran nombre d'empreses tecnològiques arran de la ràpida proliferació del sector de la ciberseguretat, no es pot perdre de vista el paper d'empreses israelianes com NSO Group,[1] que van revolucionar aquest mercat, encara emergent l'any 2010. NSO Group va ser la primera empresa capaç de desenvolupar una tecnologia d'espionatge amb propietats inèdites, com tenir accés i control total del contingut d'un dispositiu mòbil a distància sense el permís ni coneixement de la propietària del dispositiu. Això implica l'accés a tot el contingut del telèfon —tant de manera retrospectiva com prospectiva—, però també el control sobre la càmera i el micròfon.

Lluny de poder considerar Pegasus com una tecnologia obsoleta, empreses com NSO Group continuen treballant per perfeccionar i modificar les propietats dels seus productes amb la finalitat d'assolir l'objectiu inicial que va donar lloc a l'empresa: "desenvolupar una eina capaç de penetrar un dispositiu mòbil de manera remota i indetectable". Niv Carmi, Shalev Hulio i Omri Lavie[2] justificaven la importància de la tecnologia que havien desenvolupat assenyalant i apel·lant, des de l'inici, a una necessitat de seguretat europea: "forces policials i agències d'intel·ligència d'Europa ens van dir que, amb la tecnologia que havíem desenvolupat, podríem ajudar a resoldre el seu problema".[3] Segons la informació publicada a la seva pàgina web corporativa, l'empresa "desenvolupa la millor tecnologia de vigilància per ajudar a organismes governamentals a detectar i prevenir el terrorisme i la deliqüència".[4] Aquest element va ser el punt de partida que els va portar a fundar NSO Group Technologies Ltd. el 25 de gener de 2010.

Tot i que NSO desenvolupa un ampli ventall de productes, el seu producte més conegut és "Pegasus", una tecnologia de vigilància que —segons l'empresa— només es ven a Estats i agències d'intel·ligència a escala internacional.[5] L'evolució de Pegasus ha estat constant en els darrers anys: ha passat de requerir la interacció de l'usuari per a la seva activació a incorporar mecanismes d'explotació de tipus *zero-click* i funcionalitats com la fabricació, modificació i inserció d'informació en el dispositiu.[6] Aquesta progressiva sofisticació comporta conseqüències greus, ja que el *software* atorga un accés i un control total i desproporcionat sobre el contingut dels dispositius mòbils.

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 Més informació a la pàgina web de NSO Group, disponible a: 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/

Des del 2010 fins a l'actualitat, i en particular des del 2015, quan se'n documenta el seu primer ús per part del govern mexicà i, poc després, el govern espanyol,[7] l'empresa ha operat sota una regulació ambigua que ha permès una vigilància desproporcionada i sistemàtica de desenes de milers de persones arreu del món.[8] Així, s'ha convertit en una eina creada, provada i desenvolupada en un context d'ocupació i colonialisme a Palestina, que s'ofereix, es publicita i es comercialitza com un instrument de repressió i persecució de la dissidència al món.

Des de l'inici del genocidi d'Israel a la Franja de Gaza, NSO Group ha continuat apareixent de manera recurrent als mitjans, amb l'objectiu d'impulsar una estratègia de rentada reputacional després d'anys d'escàndols i denúncies públiques. A l'Estat espanyol s'han acumulat una desena de querelles per l'espionatge il·legal amb Pegasus d'ençà que, l'abril de 2022, un informe de The Citizen Lab[9] va corroborar el perill plantejat per una notificació de WhatsApp a 1.400 persones usuàries.[10] Entre aquestes usuàries s'hi trobaven l'expresident del Parlament de Catalunya, Roger Torrent, i l'ex diputat d'ERC, Ernest Maragall, que es van querellar per l'ús de Pegasus el 2020 contra el CNI i NSO Group.[11]

L'informe de The Citizen Lab, confirmat pel laboratori forense d'Amnistia Internacional, identificava almenys 65 persones relacionades amb el moviment independentista i per l'autodeterminació de Catalunya com a objectius de l'espionatge amb Pegasus i Candiru; entre elles, advocades, periodistes, defensores de drets humans i representants polítiques al Parlament de Catalunya i al Parlament Europeu. Un d'aquests casos s'ha convertit en la primera denúncia d'una persona afectada amb Pegasus que ha aconseguit la imputació de tres càrrecs directius de l'empresa NSO Group a Israel i Luxemburg,[12] entre ells dos dels seus fundadors, Shalev Hulio i Omri Lavie, que es troben actualment investigats en una causa penal en un jutjat de Barcelona.

7 El Diario.es (2025). *Artur Mas fue el primer espiado con Pegasus en España cuando era president 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 Project*, 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/

Des dels seus inicis, NSO Group ha destacat que la seva tecnologia té origen directe en l'experiència militar israeliana. Com prova l'informe "Les portes de entrada de la tecnologia del genocidi a Europa", és habitual que els fundadors d'empreses d'aquest sector provinguin d'unitats d'intel·ligència de l'exèrcit israelià, com ara la Unitat 8200, la Unitat 81 o el Mossad. En aquest cas, el creador tècnic de NSO Group, Niv Carmi (la N de NSO), havia estat agent d'intel·ligència i expert en seguretat del Mosaad.[13] Un cas recent, del mateix sector de mercat i que respon a la mateixa lògica és el cas de Paragon Solutions,[14] fundada a Israel el 2019 per Ehud Barak, exministre israelià, i Ehud Schneorson, excomandant de la Unitat 8200. El producte principal d'aquesta empresa és Graphite,[15] un programari espia amb capacitats tècniques[16] equiparables a les de Pegasus, protagonista de l'últim escàndol amb programari espia a Itàlia.[17]

Tal com decreta la llei israeliana en matèria d'exportació de "productes de defensa", l'Agència de Control d'Exportació de Defensa (DECA) —competència del Ministeri de Defensa d'Israel— és l'autoritat encarregada de l'exportació de llicències d'empreses com NSO Group,[18] sent l'únic responsable de supervisar i controlar la comercialització d'aquesta tecnologia amb finalitats lucratives a escala mundial. Si bé aquesta autorització és, alhora, l'argument al qual l'empresa recorre per justificar l'existència d'un suposat mecanisme de control extern, evidencia la seva relació directa amb el govern d'Israel.

NSO Group i el govern israelià: una aliança lucrativa.

Després de 15 anys d'activitat, nombrosos articles i estudis demostren com NSO Group s'ha convertit en un símbol de la indústria cibernètica ofensiva d'Israel, públicament publicitada com una eina d'exportació estratègica al servei del govern. Comercialitzat sota el segell d'"alta tecnologia de defensa feta a Israel", Pegasus ha estat promogut com un instrument central de la política exterior israeliana per reforçar, ampliar i consolidar re-

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). *Italian 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*. 7, https://www.nsogroup.com/wp-content/uploads/2025/02/2024-Transparency-and-Responsibility-Report.pdf

lacions diplomàtiques. Aquesta activitat ha anat acompanyada d'una campanya de legitimació pública, articulada al voltant de quatre eixos —securitització, normalització, neteja ètica (*ethics washing*) i el patriotisme sionista—[19] que presenten la vigilància com l'única resposta viable als reptes de seguretat.[20] Aquest és un argument recurrent, utilitzat també en el procés de desregulació i simplificació europeu, per justificar no només aquestes eines, sinó la seva mateixa existència, normalitzant-la com a inevitable en nom de la innovació.

Aquesta dinàmica ha generat un intercanvi clar: beneficis econòmics per a l'empresa i capacitat d'influència geopolítica per a Israel. Diverses investigacions han demostrat una correlació directa entre visites o reunions de caps d'estat amb representants del govern israelià i l'autorització de noves llicències d'exportació de Pegasus. Aquest patró s'ha repetit tant en processos de normalització diplomàtica, com a moneda d'intercanvi per millorar les relacions diplomàtiques amb el govern d'Israel —com en els casos d'Hongria, Polònia, Ruanda, Azerbaidjan o l'Índia—,[21] com en negociacions polítiques internacionals, incloent-hi votacions a les Nacions Unides, com en el cas de Mèxic i Panamà.[22]

En el cas de Panamà, una investigació conjunta de l'Organised Crime and Corruption Reporting Project (CCPR) —soci de Forbidden Stories—, Código Morse i Shomrim[23] ha aportat un nou element que fa visible aquesta relació de dependència entre l'empresa i el govern d'Israel. Segons la investigació, publicada el 16 de juliol de 2026, Shalev Hulio, un dels fundadors de NSO Group, hauria fet servir un passaport diplomàtic israelià per entrar a Panamà el 3 de desembre de 2013. Segons els registres migratoris paramenys, Hulio hauria entrat al país com a "diplomàtic" en una visita que ell mateix va qualificar de "recreativa", i hauria declarat a les autoritats d'immigració que s'allotjaria a l'ambaixada d'Israel. Un any abans, el 2012, el govern de Panamà hauria signat un contracte amb NSO en un procés liderat pel mateix Hulio.

L'exdirectiu de NSO ha negat aquestes informacions, però diverses persones expertes consideren que la investigació torna a posar el focus en la possible relació entre tots dos actors. L'advocat israelià Eitay Mack, conegut per la seva llarga trajectòria contra l'ús de

19 Kotliar, D. M., & Carmi, E. (2023). Keeping Pegasus on the wing: legitimizing cyber espionage. I*nformation, 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

Pegasus, ho resumeix: "[Pegasus] és una eina important perquè Israel construeixi vincles, especialment amb les unitats d'intel·ligència de països estangers [...]. És una de les seves principals eines per crear i mantenir relacions exteriors."[24]

En els darrers anys, l'exportació i la comercialització de Pegasus també ha jugat un paper destacat en la normalització de les relacions d'Israel amb diversos països del Golf[25] i en el marc dels Acords d'Abraham de 2020,[26] amb l'objectiu d'assegurar el suport diplomàtic a Israel de les nacions àrabs. El grau d'influència del govern israelià sobre l'empresa és tal que, fins i tot després que NSO Group trenqués el contracte de Pegasus a l'Aràbia Saudí per la presumpta implicació en l'assassinat del columnista del *Washington Post* Jamal

Khashoggi —al consolat saudita d'Istambul el 2018—, l'autorització va ser restablerta[27] poc després d'una trucada entre el príncep hereu Mohammed bin Salman i Benjamin Netanyahu.

El poder d'influència de Pegasus, es va posar també en evidència per una publicació de l'ambaixador israelià en funcions a la xarxa social X, en què amenaçava el govern de Pedro Sánchez amb utilitzar i publicar tota la informació relativa al cas Pegasus a l'Estat espanyol.[28] Tot i que la publicació ha estat esborrada, alguns mitjans ho van documentar i en queda constància avui dia.[29] Aquesta publicació tenia lloc hores després que el president reconegués l'estat palestí.

Espiar, criminalitzar i silenciar: Pegasus a Palestina.

Tot i que Pegasus és el cas més conegut, només és la punta de l'iceberg en l'exportació de tecnologia de cibervigilància israeliana utilitzada per al control autoritari arreu del món.

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 Els Acords d'Abraham són un conjunt d'acords bilaterals impulsats pels Estats Units durant la primera administració Trump, amb l'objectiu de normalitzar les relacions diplomàtiques entre Israel i diversos països àrabs. El primer acord es va signar el 15 de setembre de 2020 entre Israel, els Emirats Àrabs Units i Bahrain. Posteriorment, s'hi van afegir el Sudan (octubre de 2020) i el Marroc (desembre de 2020). Aquests acords representen la primera normalització formal de les relacions àrabs-israelianes des del tractat de pau entre Israel i Jordània de 1994 i l'acord entre Egipte i 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 L'ús de Pegasus a l'Estat espanyol s'ha identificat a través de dos casos diferenciats. El primer és el que es recull en aquest informe, referent al Catalan Gate; el segon afecta representants polítics de l'actual govern espanyol, cas en què s'assenyalava el Marroc com a presumpte autor de l'espionatge.

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

Sovint s'oblida que aquests sistemes s'han dissenyat i provat en el context del règim d'ocupació, colonialisme i apartheid a Palestina, i que també s'han emprat per sabotejar i criminalitzar organitzacions palestines de drets humans. El novembre de 2021, poc després que sis organitzacions palestines de drets humans fossin designades per Israel com a "terroristes",[30] es va descobrir que sis persones que hi treballaven havien estat espiades amb Pegasus.[31]

L'espionatge contribueix al cicle de criminalització i pretén silenciar entitats com Al-Haq, Addameer o el Bisan Center, que des de fa anys documenten i denuncien els crims de guerra i de lesa humanitat comesos per Israel contra el poble palestí. Les conseqüències per a les persones palestines afectades van molt més enllà de la simple il·legalització de la seva feina. En el cas del defensor dels drets humans Salah Hamouri,[32] fou empresonat i posteriorment deportat a França,[33] sense possibilitat de tornar a Palestina ni de continuar exercint la seva tasca com a advocat als tribunals militars israelians.

Pegasus a l'ombra del genocidi.

La vinculació amb determinats nuclis militars i d'intel·ligència d'Israel forma part d'una estratègia d'Estat orientada a projectar prestigi i a reforçar la percepció de qualitat tecnològica dels productes oferts. Aquesta estratègia comunicativa s'ha vist especialment accentuada des de l'inici del genocidi a la Franja de Gaza, moment en què les empreses tecnològiques vinculades al complex militar israelià han reforçat el discurs que associa la seva experiència en contextos de "seguretat nacional" amb l'eficàcia i la fiabilitat dels seus productes. Aquesta ha estat la tesi principal de NSO Group per intentar reintroduir-se al mercat nord-americà després d'haver estat inclosa a la denominada llista de sancions del Departament de Comerç dels Estats Units,[34] el 3 de novembre de 2021, sota la justificació de "situar els drets humans al centre de la política exterior dels Estats Units".[35]

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

34 The Intercept (2023). I*sraeli 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.

Des de l'octubre de 2023, NSO Group —juntament amb una llarga llista empreses israelianes de ciberseguretat— es va oferir voluntàriament per col·laborar en la missió de localitzar els ostatges israelians.[36] De facto, NSO Group va iniciar un procés d'actualització de la seva tecnologia militar de vigilància amb l'objectiu d'atendre aquesta necessitat. Tot i l'alta competència del mercat, des del 7 d'octubre aquestes empreses estarien col·laborant en un esforç conjunt, sense precedents, per donar suport a un front comú d'"intel·ligència" digital, que ha reforçat la promoció de la tecnologia israeliana com a única al món. Organitzacions internacionals com Democracy for the Arab World Now (DAWN) han descrit aquests moviments com "un intent de l'empresa per rehabilitar la seva imatge en plena crisis",[37] una estratègia per guanyar-se la simpatia de l'actual govern nord-americà i tornar a operar en el seu mercat.

A partir d'octubre de 2023 queda palès que, en un desplegament bèl·lic sense precedents, el govern israelià torna a permetre que NSO assumeixi un paper rellevant i destacat. En un pòdcast del mitjà de comunicació israelià Haaretz, publicat el 19 d'octubre de 2023[38] —format que, segons diversos analistes, està subjecte a menys censura que la premsa escrita a Israel—, s'analitza com NSO es posa al servei del govern, assumint tasques significatives per al Ministeri de Defensa. Un fet que, lluny de ser excepcional o innovador, posa de manifest la continuïtat de la col·laboració històrica entre l'empresa i el govern d'Israel. Tot això va anar acompanyat de l'anunci, el gener de 2024,[39] del trasllat de la seu de NSO Group a unes oficines més grans, com a part d'un pla d'expansió corporativa.

Actualment, no es coneix amb certesa fins a quin punt ni de quina manera s'està utilitzant Pegasus a la Franja de Gaza. El que sí que és clar és que les forces d'ocupació israelianes hi despleguen tot el seu arsenal tecnològic, com reafirma aquest informe. Mitjans d'investigació com la revista +972 Magazine[40] han alertat sobre una eina específica basada en intel·ligència artificial destinada a elaborar llistes de possibles "objectius" militars. Aquest sistema analitza i creua grans volums de dades amb molta rapidesa i identifica milers de persones o llocs —com ara habitatges— per ser bombardejats. En el cas de Lavender —descrit com la màquina d'intel·ligència artificial que dirigeix els bombardejos

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). *Israeli 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/

d'Israel a la Franja de Gaza—[41] la verificació inclou la ubicació dels telèfons o enregistraments de veu per determinar si la persona és home o dona; sent l'únic procediment que permet al sistema confirmar que el dispositiu correspon a la persona assenyalada. Atès que Pegasus permet accedir i controlar a distància un dispositiu mòbil —incloent-hi la geolocalització i l'activació del micròfon—, experts internacionals han assenyalat que les capacitats d'aquest programari han tingut un paper crític i fonamental en l'obtenció de dades a la Franja de Gaza durant el genocidi en curs,[42] en el marc d'allò que s'ha descrit com una "fàbrica d'assassinats en massa".[43]

NSO Group a Europa, amb epicentre a Luxemburg.

Si bé l'empresa justifica el seu producte per raons de "seguretat nacional", les dades disponibles mostren centenars de milers de casos en què aquesta tecnologia s'ha utilitzat contra actors de la societat civil[44] que no representaven cap amenaça per als estats implicats. Aquestes pràctiques fomenten la construcció d'un "futurible delictiu", és a dir, la presumpta existència d'una amenaça sense fonament, un mecanisme habitual en l'ús de tecnologies de vigilància. Davant aquesta situació, nombroses organitzacions internacionals han demanat la prohibició de Pegasus.[45]

Tot i que NSO Group Technologies Ltd. és una societat privada incorporada i registrada a Israel, el nom "NSO Group" s'utilitza com a marca paraigua per designar el conjunt d'empreses associades, tant operatives com financeres, distribuïdes arreu del món. L'estructura corporativa de NSO[46] reflecteix la ràpida expansió i proliferació d'aquest sector, i adverteix d'una realitat preocupant en l'actualitat.[47] Amb un total de 13 societats *holding* i 12 filials en múltiples jurisdiccions, el grup opera mitjançant una estructura dendrítica i deliberadament opaca, en què les empreses sovint canvien estratègicament de nom i amplien les seves activitats a altres jurisdiccions per eludir regulacions més es-

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). T*he Pegasus Project, Global Democracy under cyber attack*, https://forbiddenstories.org/about-the-pegasus-project/

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

46 La marca comercial "NSO Group" és propietat exclusiva de l'empresa matriu israeliana NSO Group Technologies Ltd.

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

trictes.[48] És per això que resulta fonamental analitzar com s'introdueix i actua a Europa com un mirall de pràctiques i lògiques que es reprodueixen dins el mercat de la vigilància. Un element estructural d'aquest tipus d'empreses és la manca de transparència i de mecanismes efectius de rendició de comptes sobre les seves activitats i exportacions, fet que dificulta l'accés a informació verificable, incloses les causes judicials iniciades per persones espiades amb Pegasus.[49]

L'entramat empresarial de NSO compta amb una presència especialment significativa a Luxemburg. Luxemburg, membre fundador de la UE i de la zona euro, s'ha consolidat com un *hub* estratègic per a empreses internacionals gràcies a l'accés al mercat europeu, un marc empresarial flexible, infraestructures tecnològiques avançades, estabilitat econòmica i una especialització destacada en ciberseguretat, i és activament promogut a Israel com a destinació per a l'expansió empresarial.[50] En el moment de redacció d'aquest informe, NSO hi té dinou societats domiciliades, onze de les quals comparteixen el mateix objecte social.[51] Aquesta estructura corporativa amplia el ventall d'actuació d'aquestes entitats, atorgant-los un caràcter instrumental, ja que amplia el seu àmbit d'actuació sense definir-ne amb claredat la finalitat. A més, les societats comparteixen no només l'objecte social sinó també la ubicació física.[52]

L'informe final de la Comissió PEGA del Parlament Europeu,[53] va concloure que el manteniment de NSO depèn en part del suport de les societats establertes a Luxemburg. L'informe identificava aquestes entitats com el centre de negocis europeu del grup, que facilita la seva activitat amb una regulació menys estricta tant dins de la UE com en tercers països, i gestiona facturació, contractes i pagaments vinculats al programari espia.[54] La permissivitat de la UE envers el mercat de programari espia comercial no només afavoreix

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 L'objecte social d'onze d'aquestes societats és ser designades formalment —mitjançant contracte, acord social o decisió d'un òrgan competent— per exercir càrrecs o funcions en altres societats, i actuar com a sòcies directores generals, adquirir participacions a Luxemburg o a l'estranger i intervenir en la seva gestió.

52 De les dinou societats de NSO Group a Luxemburg catorze tenen el mateix domicili social, mentre que les cinc restants es troben concentrades en una altra adreça

53 Durant un any va investigar els casos d'espionatges amb Pegasus a la Unió Europea amb especial atenció a Hongria, Polònia, Grècia i l'Estat espanyol. Més informació a: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/761472/IPOL_BRI(2024)761472_EN.pdf

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

que aquestes empreses operin sota un marc normatiu més lax, sinó que també dota de legitimitat la comercialització dels seus productes des de territori europeu.

Entre les dinou societats vinculades a NSO Group registrades a Luxemburg, destaquen Osy Technologies Sàrl i Q Cyber Technologies Sàrl, tant pel seu vincle amb l'ús de programari espia com per la seva rellevància estructural dins del grup. Osy Technologies, creada el febrer de 2014, va ser la primera societat del grup al país, seguida de Q Cyber Technologies, constituïda el gener de 2016 amb Osy com a accionista únic. Ambdues se situen en el nucli originari de la presència europea del grup, que es va consolidar posteriorment mitjançant una ràpida expansió societària —tres el 2017, quatre el 2018 i cinc el 2020. Osy i Q Cyber mantenen llaços directes amb NSO Group Technologies, fins al punt de compartir junta directiva en els primers anys. Dos dels fundadors d'NSO, Omri Lavie i Shalev Hulio, hi tenen una presència destacada.[55]

Segons la justícia israeliana, aquesta estructura també tindria una finalitat fiscal. L'agost de 2026, un tribunal israelià va condemnar NSO Group per frau. Segons la sentència, entre 2014 i 2018 el grup va rebre 86 milions de dòlars en beneficis a través d'Osy sense pagar els impostos corresponents a Israel.[56] El tribunal també va concloure que l'estructura de propietat d'NSO a través d'Osy es va crear, almenys en part, per reduir els impostos de les seves operacions d'endeutament i finançament.

A més de l'objectiu fiscal, la presència a Luxemburg també ha servit per construir una nova imatge.

Cal destacar que, quan el 14 de febrer de 2019 l'equip directiu i fundador d'NSO Group va anunciar que la firma de capital privat britànica Novalpina Capital n'assumia el control, el grup ja es presentava com una "empresa de tecnologia cibernètica amb seu a Luxemburg", resultat de la "fusió d'empreses de tecnologia cibernètica israelianes i europees".[57] Aquesta presentació no només pretenia reformular la identitat corporativa del grup sota una aparença més europea, sinó que també responia a una estratègia de posicionament institucional orientada a legitimar la seva activitat dins del mercat europeu de la ciberseguretat i a distanciar-se parcialment de la seva vinculació directa amb Israel, especialment arran de les controvèrsies generades per l'ús de Pegasus. No obstant això, aquesta línia identitària més difusa, que permet un accés més permeable al mercat mundial, xoca amb els valors fundacionals del grup, reafirmats després de l'octubre de 2023, quan el grup va tancar files amb el govern israelià.

55 Lavie apareix en nou juntes directives de societats luxemburgueses i Hulio en sis, reforçant la idea d'una estructura interconnectada i 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/

Arran dels escàndols de Pegasus, a mitjan 2022, Shalev Hulio va dimitir com a CEO de NSO Group i va ser substituït per Yaron Shohat. El gener de 2023, Hulio va fundar *Dream Security*.[58] El 7 de novembre de 2023, des de la Franja de Gaza des d'on servia com a reservista israelià, Hulio va anunciar una ronda de finançament,[59] que va presentar com un "gran missatge per la comunitat tecnològica i pel poble d'Israel".[60] Tot i els seus intents de desvincular-se de NSO Group, una dotzena d'antics alts càrrecs i operatius l'han seguit a *Dream Security*, on la majoria del personal té base a Israel, malgrat disposar d'oficines a Tel Aviv, Viena i Abu Dhabi. La companyia ha nascut envoltada de controvèrsia pels seus vincles amb la dreta israeliana i internacional, especialment per la participació com a co-fundador de l'excanceller austríac Sebastian Kurz.[61] En la seva ràpida expansió, *Dream Security* segueix el rastre de NSO Group, tot mantenint una presència destacada a Europa.

WhatsApp vs. NSO Group i la responsabilitat de l'empresa.

La denúncia presentada per WhatsApp i Meta contra NSO Group el 2019 als Estats Units[62] va marcar un punt d'inflexió en la crisi reputacional de l'empresa. Durant el procés, el Departament de Comerç nord-americà va incloure NSO Group a la seva llista de sancions el 2021,[63] en considerar que les seves activitats contravenien els interessos de seguretat nacional. Des d'aleshores, NSO Group se li prohibeix operar al mercat estatunidenc i el seu personal té restringit l'accés al país.[64] Malgrat l'impacte econòmic i polític d'aquesta sanció, la Unió Europea no ha adoptat mesures equivalents ni ha establert una posició comuna sobre la prohibició de Pegasus.

El desembre de 2024, un tribunal de Califòrnia va condemnar NSO Group per vulnerar lleis federals i estatals de frau i abús informàtic, a favor de WhatsApp,[65] imposant una indem-

58 Dream Security és una start-up dedicada a solucions defensives de ciberseguretat per a infraestructures crítiques, amb l'ambició pública de convertir-se en la "millor plataforma defensiva de ciberseguretat basada en intel·ligència artificial del món". Més informació disponible a: 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). W*hatsApp 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

65 Sentència procediment WhatsApp v. NSO Group (2024). Per a més informació consulta: https://www.documentcloud.org/documents/25467209-gov/

nització superior als 168 milions de dòlars.[66] El procediment també va tornar a posar de manifest l'opacitat del grup i va demostrar que és NSO Group qui realitza les fases inicials d'infecció i extracció de dades dels dispositius atacats, contrariant així el relat que havia mantingut fins ara,[67] segons el qual negava la seva participació en el procés d'infecció. La sentència ha estat celebrada internacionalment com una fita clau en la lluita contra els abusos dels programes espia.[68]

Reorientació estratègica cap a l'americanització de NSO Group

Tot i la reubicació de desenes de treballadores arran de la crisi reputacional de NSO Group, l'empresa va continuar operant —fins a novembre de 2025— sota el lideratge d'un dels seus fundadors, Omri Lavie. Després de 25 anys d'activitat i amb més de 22 clients només a Europa —incloent-hi 12 dels 27 estats membre—,[69] el novembre de 2025 es va produir un canvi substancial en la direcció. Per primera vegada, els fundadors —alguns actius des de 2010— van deixar de tenir-hi qualsevol participació, fet que marca un punt d'inflexió en la trajectòria de l'empresa.

La nova etapa, encapçalada per l'advocat nord-americà David Friedman,[70] coincideix amb l'adquisició total de la companyia per un grup d'inversors dels Estats Units —alguns amb nacionalitat israeliana—, fet que posa de manifest la seva connexió amb el govern israelià i amb sectors de l'extrema dreta. L'actual president executiu va ser l'ambaixador dels EUA a Israel durant la primera administració Trump i va participar en la negociació dels Acords d'Abraham. També destaca per les seves intervencions públiques en defensa dels assentaments il·legals al Territori Palestí Ocupat i per impulsar campanyes de finançament destinades a aquest objectiu. Aquest canvi en la direcció i la propietat s'emmarca en una tendència d'americanització de NSO Group, en què un dels objectius és aconseguir l'aixecament de la sanció per tornar a operar al mercat nord-americà.

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

Aquest canvi marca un nou rumb per al grup empresarial: sobre el paper ara és una empresa nord-americana, però continua operant de manera efectiva des d'Israel. Aquest també és el cas de Paragon, que el desembre de 2024 es va fusionar amb REDLattice,[71] una empresa nord-americana de ciberseguretat ofensiva propietat del fons AE Industrial Partners. També és el cas de Candiru, adquirida per la firma d'inversió nord-americana Integrity Partners.[72] Ara, totes tres empreses competeixen per obtenir contractes als Estats Units, tot i les sancions imposades.

En el context actual, un nombre creixent d'empreses israelianes està optant per traslladar-se o obrir filial a Europa —una pràctica ja present des de fa anys, però actualment intensificada—, atreta per un entorn legislatiu més permissiu que facilita la proliferació i l'expansió del mercat europeu de programari espia comercial.[73]

Paral·lelament, el canvi de direcció i de propietat ha comportat modificacions en tres societats d'NSO Group registrades a Luxemburg[74] passen a ser dirigides per Ohad Shazar Shalem Schremer.[75] L'advocat israelià resideix a l'assentament il·legal de Neve Daniel, a Gush Etzion, dins del Territori Palestí Ocupat, i forma part de la junta directiva d'una associació de colons. Aquest nou lideratge reflecteix una orientació corporativa alineada amb l'extrema dreta —tant a Israel com a escala internacional— i amb interessos de caràcter 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 Per més informació, anar a l'apartat IV.2 (pàgina 37) sobre el marc regulatori Europeu.

74 Les tres societats de NSO Group a Luxemburg que canvien de direcció són: NorthPole Newco, Osy Technologies i Q Cyber Technologies.

75 Ibid.