DESINFORMACIÓN E INSTRUMENTALIZACION DE INSTITUCIONES ACADEMICAS, POLITICAS Y PRENSA: EL CASO CATALANGATE

JOSÉ JAVIER OLIVAS OSUNA

Investigador Senior Programa Atracción de Talento Investigador, Departamento de Ciencias Políticas y Administración, Universidad Nacional de Educación a Distancia (UNED). Investigador Asociado en LSE IDEAS, Then London School of Economics and Political Science (LSE).

Este capítulo resume algunos de las razones por las que el análisis de la desinformación se ha convertido en una prioridad en varias disciplinas académicas aludiendo a varias de sus manifestaciones y a como es utilizada como herramienta política. A continuación, se desgrana el caso CatalanGate sobre presunto ciber-espionaje ilegal que constituye un ejemplo paradigmático de como una variedad de actores con intereses más o menos sinérgicos, incluyendo instituciones académicas, grupos políticos y medios de comunicación, colaboran en la generación y propagación de un escándalo que pivota en informaciones no verificables y sesgadas. Es capítulo trata tanto el origen de esta campaña, gracias a unas filtraciones a la prensa del supuesto espionaje a algunos líderes independentistas en 2020, como su relanzamiento en 2022 con la publicación de un polémico informe por Citizen Lab que a pesar de graves problemas metodológicos y éticos, consigue enorme repercusión mediática e dañar la imagen de España. El capítulo finaliza destacando su impacto negativo a nivel de confianza y erosión institucional y señalando la importancia de la transparencia y la rendición de cuentas como mecanismo para mitigar el problema de la desinformación.

1. LA ERA DE LA DESINFORMACIÓN

El término desinformación se refiere a la diseminación deliberada de información falsa para condicionar opiniones y actitudes (Fetzer 2004). La vigencia de este fenómeno y la atención mediática y académica creció de una forma exponencial a partir de 2016 en torno a las elecciones presidenciales que ganó Donald Trump y al referéndum sobre el «Brexit» (Kapantai et al. 2021). Muchos analistas atribuyeron a las «fake news» (noticias falsas) un gran impacto en los resultados de ambas votaciones. Más tarde, a raíz de la gran cantidad de desinformación que circuló asociada a la pandemia de la COVID19, se popularizó el término «infodemia» en referencia a la epidemia de ruido informativo e información engañosa que se expandió sobre todo en los primeros meses de la crisis (Eysenbach 2009; Gallotti et al. 2020). El análisis de la desinformación se expande a

través de muchas áreas de investigación (psicología, ciencias de la información, informática, ciencias políticas, comunicación, marketing, pedagogía, economía, etc.) y por tanto existe una gran variedad en sus enfoques. Algunos estudios se centran más en los procesos o canales de diseminación, otros en los resultados o impactos de estas campañas, en la fabricación de legitimidades o bien en las actitudes que posibilitan el éxito de la desinformación o que esta estimula (Di Domenico et al. 2021).

Dentro de la desinformación se pueden distinguir una amplia variedad de técnicas para condicionar al individuo entre las que destacan la fabricación de información, la manipulación de contenidos, contenido impostor, engañoso o descontextualizado, la sátira y las falsedades profundas o «deep fakes» (House of Commons 2018). A veces contenido presuntamente inocuo como una parodia, una broma o una noticia con parte de contenido verificable tienen más potencial de desviar la atención de los hechos y predisponer a la audiencia que una mentira. Mientras que la deliberación reduce la creencia en la información falsa y sesgada (Bago et al. 2020), la sobrecarga cognitiva, la falta de tiempo para la reflexión, la repetición, la polarización política y el sesgo de confirmación hacen a los ciudadanos más vulnerables a ésta (Kapantai et al. 2021; Gwebu et al. 2022). Incluso las organizaciones que presuntamente defienden a los ciudadanos de las manipulaciones informativas, como las famosas verificadoras de datos o «fact-checkers», acaban a menudo siendo víctimas de sesgos y contribuyendo a reforzar ciertas posturas no imparciales (Fernández-Roldán et al. 2023).

En los últimos años han surgido varias iniciativas internacionales para combatir la desinformación y el daño que causa a las democracias, algunas coordinadas por organizaciones supranacionales como la Comisión Europea, OCDE y Naciones Unidas (European Commission 2018; UN 2022; OECD 2023). Estudios académicos muestran como la desinformación se usa para condicionar el voto en citas electorales, para cuestionar la integridad de resultados de electorales, para generar actitudes xenófobas, para erosionar la confianza en gobiernos e instituciones democráticas (Kapantai et al. 2021). La información falseada se instrumentaliza a menudo con fines no políticos pero que también tiene un fuerte impacto a nivel de políticas públicas y por lo tanto deben ser tenidas en cuenta por nuestros gobernantes. Se fabrican bulos y teorías conspirativas respecto al uso de vacunas, utilización de servicios públicos por parte de inmigrantes o incluso atentados terroristas (Douglas et al. 2019).

Aunque la desinformación ha sido una herramienta política clave ya desde tiempos de imperio romano, es ahora en el siglo XXI cuando estamos atravesando una crisis sin precedentes y cuando muchos gobiernos y actores políticos se han lanzado a una especie de carrera armamentística de desinformación (Posetti & Matthews 2018). Las operaciones de desinformación se aprovechan de las debilidades estructurales del sistema de medios de comunicación tradicionales (Benkler et al. 2018). Gracias a las nuevas tecnologías de la información estamos siendo testigos de un proceso que en inglés es conocido como «weaponization» es decir la transformación de la información falaz en un arma que se puede usar tanto en conflictos políticos, como en actividades criminales y guerras (UNIDIR 2018, Brown 2020). Los recientes conflictos en Ucrania y Palestina muestran el poder de la desinformación como arma de guerra.

Los movimientos populistas usan desinformación para generar y socavar legitimidades, y construir un «pueblo» víctima de un «otro» que oprime o abusa del primero (Olivas Osuna 2021). Las paparruchas o «fake-news» se han convertido en herramientas cada vez más utilizadas por los partidos políticos para generar emociones negativas que unan el grupo y aumenten su indignación hacia los adversarios políticos, élites, inmigrantes o minorías etnolingüísticas o religiosas. Aunque a corto plazo estas herramientas sean bastante efectivas para culpabilizar a rivales y ocultar errores propios, a largo plazo pueden contribuir a la fragmentación de la sociedad. El creciente riesgo de polarización afectiva que sufren muchas democracias está relacionado con la manipulación de emociones a través de la desinformación (Serrano-Puche 2020).

Los nuevos formatos introducidos por las redes sociales, con comunicaciones más sucintas e inmediatas, sus algoritmos que amplifican contenidos y generan cámaras de resonancia, y el hecho que los periodistas han dejado de ejercer de filtros para contrastar la veracidad de las informaciones, han contribuido a la vulnerabilidad de nuestra sociedad ante este fenómeno (Graves & Anderson 2020). Las campañas de desinformación contribuyen a generar cinismo y polarización y a que la población cuestione la autenticidad de cualquier fuente de información. Se dificulta así la comunicación basada en los hechos, la lógica, el respeto moral y la deliberación democrática (McKay & Tenove 2021). Además, facilitan la radicalización violenta de la ciudadanía. Las teorías de la conspiración y desinformación contribuyen a satisfacer la necesidad de significancia de ciertos individuos, los aísla de personas que piensan diferente y los acerca a redes que validan narrativas que justifican la violencia (Kruglanski et al. 2022).

2. CATALANGATE: EL ORIGEN DE UNA COMPLEJA CAMPAÑA DE DESINFORMACIÓN

España ha sido el objetivo de numerosas campañas de desinformación a lo largo de su historia. Los intentos de demonizar y deslegitimar a los españoles fueron frecuentes entre los siglos XVI al XVIII cuando esta monarquía era una de las principales potenticas militares y comerciales del mundo (Keen 1969). Las informaciones falsas también jugaron un papel muy importante en Estados Unidos para justificar la guerra contra España en Cuba (Miller 2021). Durante el siglo XX la mal llamada «gripe española» y el revisionismo histórico con tintes hispanófobos de algunos líderes latinoamericanos y, ya en el siglo XXI, la caricaturización de España junto a los otros países del sur de Europa (los «PIGS») durante la Gran Recesión, son ilustrativos de maniobras de distorsión informativa que han causado prejuicio a los intereses de España.

Sin embargo, en los últimos años, debemos al movimiento independentista catalán, los mayores esfuerzos para denigrar la imagen de España al exterior. El proceso independentista ha utilizado una gran variedad de técnicas y canales de desinformación (Barberá 2021; Llorca-Asensi *et al.* 2021; Curiel *et al.* 2022). La preocupación fue tal que en 2018 el Gobierno creó la Secretaría de Estado de la España Global, para defender la reputación de España como democracia plena, y durante dos años hizo frente a la campaña de desprestigio del proceso independentista en el exterior (España Global 2019).

Entre las operaciones de comunicación del independentismo para presentar a España como un estado opresor, cabe destacar el llamado «CatalanGate» que acusa al gobierno español de haber espiado ilegalmente a políticos y miembros de la sociedad civil catalana. El inicio de este escándalo hay que buscarlo en el verano de 2020 cuando el centro de investigación *Citizen Lab* perteneciente a la *Munk School of Global Affairs and Public Policy* de la Universidad de Toronto, presuntamente detecta infecciones con el programa de vigilancia o *spyware* Pegasus en los teléfonos de varios líderes independentistas catalanes. El 13 de julio de 2020, los diarios *El País* y *The Guardian* publican simultáneamente la exclusiva sobre el ataque al teléfono del político de *Esquerra Republicana de Catalunya* (ERC) y Presidente del Parlamento de Cataluña Roger Torrent, así como a otros líderes independentistas[1].

[1] El País. El móvil del presidente del Parlament fue objetivo de un programa espía que solo pueden comprar Gobiernos. https://elpais.com/espana/2020-07-13/el-movil-del-presidente-del-parlament-fue-objetivo-de-un-programa-espia-que-solo-pueden-comprar-gobiernos.html; The Guardian. Phone of top Catalan politician 'targeted by government-grade spyware'.

Sin embargo, esta historia de espionaje a políticos catalanes genera muchas dudas por un gran número de contradicciones y detalles inusuales que emergen. En teoría, el nombre de Torrent y sus compañeros estaba en una lista que tenía WhatsApp con 1.400 usuarios presuntamente atacados con Pegasus en 2019. *New York Times* explica que fueron investigadores de Citizen Lab quienes descubrieron la presunta brecha de seguridad en esta plataforma de mensajería[2] y WhatsApp admite que Citizen Lab se había presentado voluntario para ayudarles a identificar presuntas víctimas[3]. Gracias a este trabajo de Citizen Lab recolectando evidencia de ataques de Pegasus desde mayo de 2019, WhatsApp se querelló en octubre del mismo año contra la compañía NSO Group que comercializa este spyware. No obstante, en ninguno de los informes que había elaborado previamente Citizen Lab sobre Pegasus había referencias a España, que no aparecía en el listado de 45 países donde habían encontrado o sospechaban casos de infecciones de Pegasus.[4] Tampoco en la documentación aportada por WhatsApp en su querella entre 2019 y diciembre de 2020, se mencionan presuntos ataques o víctimas en Cataluña[5].

Resulta aún más extraña la manera en que este caso llegó a la luz y cómo se enteraron las presuntas víctimas catalanas del espionaje. The Guardian explica que Citizen Lab había contactado directamente a Anna Gabriel, que se encontraba fugada de la justicia española, y Jordi Domingo, vigilado a petición de la Audiencia Nacional, había recibido una notificación de WhatsApp[6]. Sin embargo Roger Torrent, la figura central en la noticia, explica en su libro que no recibió ninguna comunicación de WhatsApp o de Citizen Lab sino que la primera notificación de su presunto ataque con Pegasus fue realizada por los periodistas Joaquín Gil (El País), Sam Jones y Stephanie Kirchgaessner (The Guardian),

---

https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware

[2] New York Times. 13/05/2019. WhatsApp Rushes to Fix Security Flaw Exposed in Hacking of Lawyer's Phone. https://www.nytimes.com/2019/05/13/technology/nso-group-whatsapp-spying.html

[3] WhatsApp. 31 de octubre 2019. FAQ. Protecting our users from a video calling cyberattack. https://web.archive.org/web/20191031150546/https://faq.whatsapp.com/help/video-calling-cyber-attack. Esta página web fue borrada posteriormente por WhatsApp.

[4] Threat Post. 18 de septiembre 2018. Dangerous Pegasus Spyware Has Spread to 45 Countries. https://threatpost.com/dangerous-pegasus-spyware-has-spread-to-45-countries/137506/

[5] CourtListener. WhatsApp Inc. v. NSO Group Technologies Limited (4:19-cv-07123) District Court, N.D. California. 27 de octubre 2023. https://www.courtlistener.com/docket/16395340/facebook-inc-v-nso-group-technologies-limited/; Case 20-16408 In the United States Court of Appeals for the Ninth Circuit. NSO Group Technologies Ltd. et al. Defendants-Appellants v. WhatsApp Inc. et al. Plaintiffs-Appelles. 21 de diciembre de 2020. https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2020/12/NSO-v.-WhatsApp-Amicus-Brief-Microsoft-et-al.-as-filed.pdf

[6] The Guardian, idem; La Razón.22 de octubre 2022 https://www.courtlistener.com/docket/16395340/facebook-inc-v-nso-group-technologies-limited/

el 8 de julio de 2020 (Torrent 2021, 14). Estos periodistas, ya en la primera reunión, insistieron en que se pusiera en contacto con Citizen Lab y mencionaron directamente a su director Ronald Deibert y al investigador John Scott-Railton. Estos periodistas nunca revelaron fuente de la filtración ni las aparentes indicaciones que acompañaron esta, pero incluso a Gil le pareció algo inhabitual la situación: «Y la primera llamada que le hice fue extraña: ¡llamar a un político para que llamara a un canadiense para decirle si había sido espiado!» (Torrent 2021, 100).

En teoría los datos de los clientes de WhatsApp no son públicos ni se pueden compartir con periodistas sin una autorización expresa. WhatsApp ha evitado responder cuando se le ha preguntado bajo que tipo de acuerdo dio permiso a Citizen Lab a analizar los datos y contactar directamente con las personas presuntamente atacadas con spyware[7]. Surge la duda si esta implicación de Citizen Lab es compatible con la política de privacidad y «end-to-end encryption» que teóricamente protege a los usuarios de WhatApp, y con Reglamento General de Protección de Datos del Parlamento Europeo y el Consejo de la Unión Europea. El 9 de julio de 2020, en su primer contacto, Scott-Railton explica a Torrent que Citizen Lab colaboraba con WhatsApp, buscando y encontrando las personas detrás de los móviles que habían sido víctimas de espionaje y que el mismo intentó ponerse en contacto con Torrent, pero sin lograrlo y que «el objetivo de toda la investigación posterior es relacionar la crisis de seguridad del incidente de WhatsApp con Pegasus» (Torrent 2021, 26). Muestran estos comentarios que el laboratorio canadiense no se regía por motivos estrictamente académicos.

Es aún más problemática la secuencia de eventos esos días que Torrent documentó al detalle en su libro. El 10 de julio Scott-Railton comienza a analizar el teléfono de Torrent de forma remota desde Toronto explicando que necesitan hacer seguimiento durante unos días, (Torrent 2021, 37-38). Sin embargo, The Guardian y El País publican la noticia el día 13, antes de que se concluyese este análisis, sorprendiendo a Torrent: «Ha salido! Hostia, han tenido miedo de que les fastidien la exclusiva y lo han publicado» (Torrent 2021, 62). Ese mismo día Gil les había dicho: «El problema es que a nosotros nos piden un mínimo de documentación para acreditar cada párrafo» (Torrent 2021, 61), pero en este caso no esperaron ni a la confirmación de WhatsApp, ni a los resultados del análisis

[7] El autor ha escrito en numerosas ocasiones a distintos responsables y cuentas oficiales de WhatsApp y no ha obtenido ninguna respuesta.

de los teléfonos. Ambos medios publicaron el artículo con graves acusaciones contra España con tan solo unos nombres en una lista filtrada.

Al día siguiente, el 14 de julio, *Le Monde* da la noticia[8] y el equipo de ERC se pone a trabajar en la estrategia de comunicación para conseguir alcanzar una mayor audiencia posible. Torrent hace una declaración institucional que es retrasmitida por TV3 donde acusa al gobierno español de espiar su teléfono, y de las que se hacen eco también *Reuters*, *The Washington Post*, *Corriere della Sera* y *Al-Jazeera* (Torrent 2021, 63-67). ERC, *Junts Per Catalunya* (JxC), Partido Nacionalista Vasco, *Bildu*, Compromis, *Bloque Nacionalista Galego*, Más País, CUP, Equo y Podemos, firman una declaración conjunta pidiendo una comisión de investigación sobre el presunto espionaje[9].

Ese mismo día empiezan a trabajar en la estrategia judicial con Andreu Van den Eynde, abogado de los líderes de ERC condenados por los hechos de 2017: «Ayudamos a Andreu a acotar el relato (...) Andreu dice que con el informe de Citizen Lab tenemos suficiente para apoyar la querella, pero que también nos gustaría tener la confirmación de WhatsApp». (...) «Bueno, ahora solo tenemos que definir a quién dirigimos la querella" (Torrent 2021, 71-72).

El 15 de julio en una reunión extraordinaria del grupo parlamentario ERC se debate la estrategia de comunicación sobre el caso de espionaje y Ernest Maragall, otra presunta víctima, insiste en que se utilice el término «Catalangate» para resaltar su supuesta semejanza con el escándalo «Watergate» (Torrent 2021, 80-81). El 16 de julio Torrent anuncia en una entrevista en la Cadena SER que él y Maragall se van a querellar contra el antiguo director de los servicios secretos españoles, Félix Sanz Roldán, por espionaje con Pegasus[10]. Pero, ese mismo día Citizen Lab comunica a ERC los resultados del análisis: «Puede confirmar al presidente Torrent que, en este momento, su teléfono no está infectado por ningún spyware ... Tengo un teléfono móvil limpio. Es tranquilizador y una decepción al mismo tiempo» (Torrente 2021, 104).

---

[8] Le Monde. Des militants catalans visés par un logiciel espion ultraperfectionné. https://www.lemonde.fr/pixels/article/2020/07/14/des-militants-catalans-vises-par-un-logiciel-espion-ultraperfectionne_6046138_4408996.html

[9] RTVE. Torrent denuncia que España practica el "espionaje político" dentro de una "causa general contra el independentismo". https://www.rtve.es/noticias/20200714/torrent-denuncia-espana-se-practica-espionaje-politico-marco-causa-general-contra-independentismo/2027952.shtml

[10] Europa Press. Torrent y Maragall se querellarán contra el exdirector del CNI Félix Sanz Roldán por el 'hackeo' de sus teléfonos, 16 de julio de 2020, https://www.europapress.es/nacional/noticia-torrent-maragall-querellarancontra-exdirector-cni-felix-sanz-roldan-hackeotelefonos-20200716100349.html

Curiosamente los resultados negativos no frenan la maquinaria legal y de comunicación puesta en marcha, ya que ambas partes tienen confianza en que encontrarán infecciones si siguen buscando. El 17 de julio, Scott-Railton sugiere a ERC contactar al abogado de la organización mejicana R3D para denunciar los ataques en los medios y los tribunales (Torrent 2021, 111). Al día siguiente Scott-Railton indica: «Su tema es la oportunidad de abrir un caso en la Unión Europea. Creo que hay suficientes elementos para hacer de su problema un problema europeo» (Torrent 2021, 23-26). La insistencia de Citizen Lab en en llevar a los tribunales no parece propia de un centro de investigación científico. 21 de julio el jefe de gabinete de Torrent, Oriol Sagrera afirma que «Scott-Railton y Campo están trabajando en el informe final del caso junto con una empresa de comunicaciones estadounidense" (Torrent 2021, 135). Tampoco es normal implicar empresas de comunicación en la redacción de informes académicos.

Sagrera se refiere a Elies Campo, un activista independentista que había asesorado a Carles Puigdemont y Quim Torra en aspectos relativos a la consecución de una República, y que se puso en contacto con Citizen Lab y ofreció voluntario para ayudarles en la investigación. Campo coordinó el trabajo de identificación de víctimas de Pegasus y aparece no solo como co-autor del informe publicado en 2022, sino además él y sus padres aparecen en el como presuntas víctimas del espionaje (Olivas Osuna 2022, 42-43, 202, 205).

El 27 de julio de 2020, Citizen Lab confirma a ERC que ninguno de los demás teléfonos que habían solicitado analizar estaba infectado (Torrent 2021, 150). A pesar de eso, ese mismo día Torrent y Maragall envían cartas a Dunja Mijatovic, Comisaria de Derechos Humanos del Consejo de Europa, a Julie Verhaar, en Amnistía Internacional, y a David Kaye, Relator Especial de las Naciones Unidas, solicitando que estas organizaciones reconociesen y denunciasen la grave situación de espionaje ilegal de España (Torrent 2021, 151-152). ERC se coordina con El País y The Guardian para que estos periódicos publiquen parte del comunicado que WhatsApp emitió a solicitud de los líderes independentistas.

El 28 de julio, The Guardian recoge el testimonio Niamh Sweeney, Directora de Asuntos Públicos de WhatsApp que, aunque confirma que los nombres de los independentistas estaban en una lista de posibles víctimas de espionaje, admite que «sobre la base de la información que disponemos, no estamos en condiciones de confirmar si el dispositivo

del Sr. Torrent se vio comprometido, ya que esto solo podía lograrse mediante un análisis forense exhaustivo del dispositivo»[11].

A pesar de todo el revuelo mediático y duras acusaciones vertidas, el centro canadiense no publica nada al respecto en los meses siguientes y el caso pierde paulatinamente interés. Esto puede ser debido a que no se encontraron pruebas claras de infecciones o a que como Citizen Lab admitió más tarde: sus métodos tienen una capacidad muy limitada de detectar infecciones de Pegasus en dispositivos Android (Scott-Railton et al. 2022). Al parecer los teléfonos de Torrent y los demás independentistas cuyos nombres aparecían en la lista original eran dispositivos Android. Ni El País ni The Guardian publicaron la información de que los resultados de los análisis fueron finalmente negativos. Torrent agradeció a esos periodistas su implicación en el lanzamiento del caso, llegando a mencionar a Joaquín Gil 29 veces en su libro.

En definitiva, en el verano de 2020 se creo un gran escándalo internacional y un grave daño reputacional a España que pivotaba simplemente en una lista de nombres que fue filtrada a unos periodistas y en unas acusaciones que no pudieron ser confirmadas por ningún análisis en ese momento. La exitosa instrumentalización de los medios de comunicación, grupos parlamentarios y organizaciones supranacionales para crear una sensación de urgencia ofreció a los políticos secesionistas catalanes la oportunidad de generar y representar una crisis política, algo similar a estrategias observadas en otros movimientos populistas en circunstancias similares (Moffitt 2015; Olivas Osuna y Rama 2021).

3. EL INFORME «CATALANGATE" DE CITIZEN LAB Y REACTIVACION DE LA CAMPAÑA EN 2022

El 18 de abril de 2022 *Citizen Lab* finalmente publica el informe «CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru» (Scott-Railton et al. 2022). Este informe, que denuncia una operación ilegal de espionaje contra el independentismo catalán, viene acompañado de una campaña de comunicación orquestada por los partidos secesionistas. Ese mismo día 18 de abril Ronan Farrow

[11] The Guardian. WhatsApp confirms Catalan politician's phone was target of 2019 attack. 28 de julio de 2020, https://www.theguardian.com/technology/2020/jul/28/whatsapp-confirms-catalan-politicians-phone-was-targetof-2019-attack

publica en *The New Yorker* un artículo acusando a España de espiar a sus ciudadanos y una semana más tarde *The Washington Post* dedica un duro editorial al caso[12].

La página «CatalanGate.cat» registrada en enero de 2022 por la Assemblea Nacional Catalana (ANC) y propiedad de Òmnium Cultural[13], ambas organizaciones independentistas, se hace eco del informe homónimo y hace un llamamiento a los ciudadanos para que presionen a la Comisión Europea para que inicie una investigación sobre España. Una cuenta de Twitter con 182.600 seguidores, utilizada durante años para promover campañas secesionistas, cambia su nombre a «@catalangate» y también se utiliza para diseminar un relato acusatorio. Los implicados llegan a afirmar que este es «el mayor caso de ciber-espionaje jamás certificado» o «el mayor el mayor caso de espionaje político conocido en Occidente»[14]. A pesar de lo sorprendente de las alegaciones, España aparece en el puesto 15 del ranking de vigilancia del National Cyber Power Index (Voo et al 2022), muchos medios de comunicación nacionales e internacionales reprodujeron durante semanas el contenido y acusaciones del informe sin un mismo atisbo de escepticismo o análisis crítico.

Se genera así otro escándalo, aún mayor que el de 2020, con graves implicaciones políticas y reputacionales para España, pero que pivota completamente sobre este informe Citizen Lab. Trabajo éste que presenta evidentes y graves problemas metodológicos e inconsistencias que pasaron desapercibidas, no solo a periodistas, sino también a políticos y otros analistas. En primer lugar, resulta extremadamente sorprendente la total ausencia de transparencia en lo relativo a, cuándo, dónde, cómo, y por quién se realizan los análisis.

Esta información no aparece en el informe, y cuando se le solicita a posteriori a Citizen Lab, estos rehuyen responder o responden con afirmaciones que no coinciden con los hechos. Por ejemplo, Deibert rechaza especificar fechas: «Las actividades de investigación comenzaron en el otoño de 2019 y continuaron hasta el momento de la

---

[12] The New Yorker. How Democracies Spy on their Citizens. 18 de abril de 2022. https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens; The Washington Post. 25 de abril. Democracies shouldn't surrender to a future of limitless surveillance. https://www.washingtonpost.com/opinions/2022/04/21/democracies-should-write-rules-spyware-not-abuse-it/

[13] Catalangate.cat. Privacitat. https://catalangate.cat/privacitat/#privacitat

[14] Jordi Sànchez. @jordisanchezp. Twitter. 18 de abril de 2022. Sinpermiso. Gonzalo Boye. CatalanGate: si se quiere, se puede. 6 de mayo de 2022. https://www.sinpermiso.info/textos/catalangate-si-se-quiere-se-puede

publicación» [15]. Es sabido que algunos teléfonos fueron estudiados en julio de 2020, como el de Torrent, y otros justo antes de la publicación. El teléfono de Jordi Solé fue analizado en marzo de 2022[16] y el de Jordi Sànchez, cuyo primer análisis había dado negativo meses atrás fue de nuevo analizado a principios de abril de 2022[17]. No hay evidencia de que ningún miembro de Citizen Lab fuese a Cataluña hasta que Campo fue contratado como *Fellow* por Citizen Lab el 1 de febrero de 2022. Su trabajo anterior no estaba cubierto por ninguna relación contractual y por tanto difícilmente sujeto al escrutinio del comité de ética investigadora de la Universidad de Toronto.

Los análisis forenses digitales remotos tienen limitaciones y se suele recomendar también análisis físicos presenciales (Krishnan et al. 2019). No hay pruebas de que ninguno de los teléfonos fuese analizado en un laboratorio, ni tampoco se explican los procesos de manipulación de la evidencia digital. De hecho, la Universidad de Toronto dice que no ha encontrado en sus registros ningún acta o documento relativo a reuniones de miembros de Citizen Lab sobre la investigación CatalanGate[18]. Además, el informe no explica cuántos teléfonos fueron analizados ni que proporción de ellos resultó mostrar indicios de ataque, siendo es básico para poder detectar errores instrumentales y la gravedad del problema. Deibert se negó a dar estos datos cuando fue preguntado formalemente[19] y en una entrevista en El País llegó a aseverar: «100% de fiabilidad de los ataques que hemos registrado» y negar la posibilidad de falsos positivos»[20]. Esto choca con la literatura académica en análisis forense digital que considera los falso positivos como una constante en esa disciplina (Alherbawi et al. 2013). Además, Citizen Lab acabó por reconocer el 22 de diciembre 2022 que se habían confundido y que no habían encontrado ataques en el teléfono del político Antoni Comín[21].

---

[15] Carta formal del director de Citizen Lab, Ronald Deibert, en respuesta a las preguntas de seis diputados al PE de Renew Europe el 13 de mayo de 2022, (carta enviada por Lorraine Ferris a Jordi Cañas publicada en la web de Citizen Lab) https://deibert.citizenlab.ca/wp-content/uploads/2022/05/2022.05.13-L-Ferris-to-J-Canas.pdf, pag. 3.
[16] The New Yorker. Ibid.
[17] Youtube. Assemblea. Jordi Sànchez #CatalanGate. 26 de abril 2022, https://youtu.be/9crBYexH6Ew
[18] Respuesta a solicitud de datos por la ley de transparencia de Ontario (FIPPA). Request #23-0029 Access Decision. 23 de junio 2022.
[19] Carta de Ronald Deibert, ibid. Pag. 4
[20] El País. Ronald Deibert, fundador de Citizen Lab: "Los gobiernos usan Pegasus porque tienen apetito de espiar". 15 de mayo de 2022. https://elpais.com/espana/2022-05-15/ronald-deibert-fundador-de-citizen-lab-los-gobiernos-usanpegasus-porque-tienen-apetito-de-espiar.html
[21] CatalanGate Report. Correcting a Case. https://citizenlab.ca/2022/12/catalangate-report-correcting-a-case/ . Comín había comparecido como víctima en la Comisión PEGA del Parlamento Europeo y sigue figurando como víctima en la página web Catalangate.cat.

El director de Citizen Lab también afirmó por escrito que «ninguna institución o grupo estuvo envuelto en el análisis forense realizado para el informe»[22]. Contradice el testimonio de Torrent que explica que ERC como JxC tenían personas analizando los teléfonos e identificando víctimas que pasaban a Campo (Torrent 2021, 142). O la declaración de Van den Eynde que asegura a la Comisión de Investigación PEGA del Parlamento Europeo que ellos tenían equipos de expertos haciendo análisis forenses junto a Citizen Lab.[23] Finalmente, Oriol Tortuella explicó que la Agència de Ciberseguretat de Catalunya (ACC), que él dirigía, colaboró estrechamente con Citizen Lab en los exámenes forenses iniciales que los partidos secesionistas ERC, JxC y CUP y las organizaciones políticas Òmnium y ANC participaban en la selección de los dispositivos que el Citizen Lab debía comprobar[24]. Tomàs Roy, el nuevo director de la ACC también confirma la colaboración con Citizen Lab desde 2020[25].

La opacidad en lo relativo a la metodología puede deberse a que el informe CatalanGate infringe muchos principios básicos de análisis forense digital de la Agencia Europea para la Ciberseguridad (ENISA), del Protocolo Berkeley para investigaciones digitales de las Naciones Unidas e incluso las directrices del National Institute of Standards and Technology (NIST) de Estados Unidos. Por ejemplo, no hay ninguna documentación o referencia a la necesaria cadena de custodia de las pruebas, ni registro de como encontraron o manejaron los dispositivos, ni si se mantuvieron aislados o desconectados de otras redes para evitar contaminación. La evidencia empírica no fue manejada exclusivamente por especialistas ya que activistas y partidos estuvieron implicados. Ni se tomaron contramedidas para evitar que la participación de Campo y otras personas con intereses políticos o personales afectase a la objetividad del informe. También sorprende que no se estudiasen varias hipótesis y se asumiese que desde un primer momento la única explicación fuese un espionaje ilegal por parte de España (ENISA 2013; Ayers et al. 2014; UN 2022b).

---

[22] Ibid. Pag.4.
[23] European Parliament Committees. PEGA: Country hearing – Spain. 29 de noviembre 2022, 9h00.
[24] La Vanguardia. La Agència de Ciberseguretat trabajó con Citizen Lab en el análisis de los móviles. 8 de mayo de 2022. https://www.lavanguardia.com/politica/20220508/8250740/agencia-ciberseguretat-trabajo-citizen-lab-analisis-moviles.amp.html
[25] Parliament.cat. Comissió d'Investigació sobre l'Espionatge de Representants Polítics, Activistes, Periodistes i llurs Familiars per part del Regne d'Espanya amb els Programes Pegasus i Candiru. 3 de noviembre 2023. https://www.parlament.cat/ext/f?p=700:DETALL_VIDEO:0:::15:P15_ID_VIDEO,P15_ID_AGRUPACIO:14801585,17489

Este incumplimiento de tantos principios básicos de análisis científico digital no impidió la publicación del informe, puesto que este no estuvo sujeto a un proceso normal de revisión de pares. En su lugar se pretendió conseguir esta apariencia dando una muestra de 4 dispositivos al equipo técnico de Amnistía Internacional que validaron la metodología. Aquí se observa otro ejemplo de mala praxis, puesto que los dos expertos en Pegasus en Amnistía, Claudio Guarnieri y Etienne Maynier, fueron antiguos empleados de Citizen Lab, el segundo tenía una doble afiliación cuando empezó la investigación en 2020[26]. Las dos organizaciones colaboran regularmente y se validan recíprocamente las metodologías (Olivas Osuna 2022, 29-34), lo que en condiciones normales las invalidaría como revisoras. Desgraciadamente tampoco es posible replicar los resultados, que sería la única justificación posible para la ausencia de una revisión formal, ya que Citizen Lab se opone a compartirlos. Además, presuntamente aconsejados por Citizen Lab, ninguno de los líderes independentistas a los que en los juzgados se les han solicitado sus teléfonos para comprobar los ataques han accedido a entregarlos para un peritaje independiente[27].

Tan preocupante resulta la negativa a revelar fuentes de financiación de Citizen Lab. Sus ingresos pasan de $871,776 dólares canadienses en 2017-2018, cuando empiezan las investigaciones sobre Pegasus a $7,769,573 en 2022-2023. Se niegan a compartir los nombres de ninguna de las organizaciones que los financian a pesar de que la ley en Ontario especifica que las universidades públicas están sujetas a las leyes de transparencia[28]. Deibert afirma que «Citizen Lab nunca ha recibido el encargo de encontrar evidencia para una demanda por parte de ninguna de las partes en ningún litigio, incluida Apple. En ninguna circunstancia emprenderíamos una investigación por encargo» y que «Citizen Lab no ha recibido nunca pagos o donaciones de Apple, WhatsApp o Facebook»[29].

Sin embargo, la evidencia parece señalar intereses económicos que Citizen Lab no ha declarado en sus trabajos. Cuando Apple se querella contra NSO, anunciaque dedicaría

---

[26] Medianama, Interview: How Amnesty Investigated The Spying Campaign Against Bhima Koregaon Activists, 19 de junio de 2020 https://www.medianama.com/2020/06/223-interview-etienne-maynier-amnesty-bhima-koregaon/ ; Claudio Guarnieri. re:publica. https://re-publica.com/en/user/11930

[27] El Triangle. Los independentistas supuestamente espiados con Pegasus se niegan a que la justicia analice sus teléfonos móviles. 3 de octubre de 2022. https://www.eltriangle.eu/es/2022/10/03/los-independentistas-supuestamente-espiados-con-pegasus-se-niegan-a-que-la-justicia-analice-sus-telefonos-moviles/

[28] Dos peticiones de transparencia han sido cursadas formalmente por el autor de esta investigación en 2022 y 2023 (peticiones #22-0052 y #23-0029).

[29] Carta de Ronald Deibert, ibid. Pags. 5-6.

10 millones de dólares a recompensar a Citizen Lab, Amnistía y otras organizaciones que le habían ayudado[30]. Más tarde Apple explica que el dinero sería canalizado a través de un comité en *Ford Foundation* y que nombra a Deibert como uno de los responsables en su asignación[31]. Las cuentas públicas de Ford Foundation demuestran los pagos a Citizen Lab, Amnistía y otras organizaciones colaboradoras[32]. Además, Sagreras ya explica a Torrent, el 21 de julio de 2020, que «Elies Campo [...] se ha puesto en contacto con John Scott-Railton y trabajarán juntos en nuestro caso. Lo hace en nombre de Apple, que también está muy interesado en aclarar quién está detrás de los ataques [...]. Los del Citizen Lab están interesados en cerrar la carpeta para que podamos suministrar munición a WhatsApp, Apple y nosotros mismos, de modo que dispongamos de material sólido que presentar ante los tribunales» (Torrent 2021, 135).

Hay que destacar también las modificaciones que llevaron a cabo en el informe, tras su publicación (Olivas Osuna 2022, 51-52). La más grave por sus implicaciones es el cambio de las presuntas fechas de inicio de infección de Van den Eynde, pasando del 14 de junio de 2020 al 14 de mayo[33]. Este adelanto en la fecha hace que el periodo de espionaje coincida con reuniones de Van den Eynde para la defensa de los líderes independentistas juzgados por los hechos de 2017. Van den Eynde declara «el mismo día que fui atacado (14 de mayo de 2020) o en torno a esa fecha tuve una reunión por vídeo-llamada, creo, con quizá diez abogados que estaban debatiendo nuestra estrategia jurídica en el caso de

[30] Apple. Apple sues NSO Group to curb the abuse of state sponsored spyware, 23 de noviembre de 2021, https://www.apple.com/uk/newsroom/2021/11/apple-suesnso-group-to-curb-the-abuse-of-state-sponsored-spyware/

[31] Apple. Apple expands industry-leading commitment to protect users from highly targeted mercenary spyware, 22 de julio de 2022, https://www.apple.com/uk/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/

[32] Ford Foundation. Governance and Financial Statements. https://www.fordfoundation.org/about/about-ford/governance-and-financial-statements/. Hay pagos relativos a actividades de ciberseguridad a Citizen Lab (1,35 millones de dólares en 2021 y 2,7 millones en 2022), a Article19 (1,125 millones de dólares en 2021 y 1 millón en 2022), Electronic Frontier Foundation (345.000 dólares en 2021 y 416.700 en 2022), Access Now (200.000 dólares en 2021 y 652.500 en 2022), Freedom of the Press Foundation (200.000 dólares en 2021 y 600.000 en 2022) y a Amnistía (200.000 dólares en 2021 y 550.000 en 2022). Estas organizaciones coinciden con las felicitadas por John Scott-Railton en un hilo en Twitter (luego borrado) por haber contribuido a buscar evidencia contra NSO para el juicio de Apple: https://threadreaderapp.com/thread/1463206324704059401.html

[33] El texto original del informe CatalanGate (18 de abril de 2022) puede consultarse en la siguiente dirección: https://web.archive.org/web/20220418110145/https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operationagainst-catalans-using-pegasus-candiru/

los políticos catalanes encarcelados» y estima que eso podría significar que se vulneró el derecho de defensa de estos lo que podría llevar a impugnar sus sentencias[34].

Finalmente hay que señalar que, el informe busca generar un estado de opinión. Aunque admite que las acusaciones se basan en «evidencia circunstancial», la selección de datos en la introducción del caso es sesgada, se oculta que muchas de las «victimas» estaban implicadas en investigaciones judiciales y que se califica como «desenfrenada, innecesaria y desproporcionada» o de «abuso» la acción de España (Scott-Railton et al. 2022). Aunque el informe habla de 65 víctimas, en esta cifra se mezclan no solo las infecciones de Pegasus, sino personas que supuestamente fueron atacadas con otro spyware (Candiru), personas que simplemente aparecían en una lista de potenciales víctimas (y cuyos teléfonos no tenían indicadores de compromiso) y otras que fueron presuntamente atacadas, pero nunca infectadas. Las entrevistas y comentarios de Deibert, Scott-Railton y Campo en prensa, televisión y redes sociales, también indican que la intención del informe es generar un estado de pánico moral e indignación contra España[35].

4. IMPLICACIONES

El mundo académico es uno de los perjudicados por el CatalanGate. Es problemático el aparente apoyo que una prestigiosa institución académica como la Universidad de Toronto, ha proporcionado (de forma voluntaria o involuntaria) a una campaña de desinformación a gran escala contra un país y sus instituciones por parte de movimiento nacionalista. La negativa a abrir una investigación interna y la reticencia a facilitar la información solicitada sobre el estudio de Citizen Lab en Cataluña choca con su política pública de rendición de cuentas y de transparencia, y puede considerarse una anomalía en una universidad considerada entre las mejores del mundo. Cuando un centro relativamente pequeño como Citizen Lab publica en un año, 2022, 15 informes (muchos con gravísimas acusaciones) (Citizen Lab 2023) y se niega a revelar sus fuentes de financiación, imposibilita la replicabilidad de sus análisis y no cumple con los mínimos

[34] European Parliament, Multimedia Centre, Committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, 28 de noviembre de 2022, https://multimedia.europarl.europa.eu/en/webstreaming/pegacommittee-meeting_20221129-0900-COMMITTEE-PEGA

[35] Por ejemplo, CCMA.Cat. TV3. Preguntes Freqüentes. El Catalangate amb John Scott-Railton i Elies Campo, Lang Lang i Noemí Casquet, 23 de abril 2022; https://www.ccma.cat/tv3/alacarta/preguntes-frequents/el-catalangate-amb-john-scott-railton-i-eliescampo-lang-lang-i-noemi-casquet/video/6155478/; CCMA.cat. TV3. Pegasus, l'espia a la butxaca. 16 octubre 2022, https://www.ccma.cat/tv3/alacarta/30-minuts/pegasus-lespia-a-la-butxaca/video/6180772/ ; Olivas Osuna (2022, 131-132).

estándares metodológicos que se exigen a las publicaciones académicas, es normal que surjan dudas y críticas en la comunidad científica, como en este caso. El abuso de la condición de centro de investigación público con fines políticos y económicos no declarados puede contribuir a la deslegitimación del trabajo de otros investigadores y a generar escepticismo en la ciudadanía.

Tres cartas distintas, firmadas por Europarlamentarios y por profesores e investigadores pidieron que la Universidad de Toronto abriese una investigación interna, pero ésta sorprendentemente rechazó hacerlo[36]. Al contrario, hubo movimientos para silenciar la investigación y las legítimas críticas vertidas. No solo se negaron a revela una gran parte de los datos solicitados por transparencia relativos a documentación y financiación, sino que se persuadió a una periodista del periódico de la Universidad de Toronto *The Varsity* que estudió durante meses el caso para que lo dejara y no publicase nada sobre el tema. Además, miembros de Citizen Lab y de las organizaciones con las que colaboran enviaron una carta difamatoria a la Comisión PEGA y a varios medios internacionales para evitar que dos investigadores que habían sido invitados a testificar a esta comisión pudieran hacer públicos los resultados de sus investigaciones que mostraban las fallas en el informe CatalanGate[37]. Los investigadores que revelaron los problemas también han sufrido acoso en redes por cuentas que promueven las investigaciones de Citizen Lab (Olivas Osuna 2022, 213-221). Mientras tanto el centro de investigación canadiense sigue publicando informes cuyos resultados no son replicables, ni revisados por pares, siguen sin declarar ningún conflicto de intereses ni fuentes de financiación. Los resultados de estos continuan siendo publicados en multitud de medios internacionales sin pasar ningún mínimo escrutinio y son usados como herramienta arrojadiza por grupos políticos y activistas.

Es destacable también la instrumentalización de instituciones políticas, y en particular de las comisiones de investigación sobre Pegasus en esta campaña. Los dos presidentes de la Comisión Pegasus del Parlamento de Cataluña, Meritxell Serret y Josep Maria Jové, y su vicepresidente, Albert Batet, son políticos independentistas y presuntas víctimas de Pegasus[38]. Una de las vicepresidentas de la Comisión PEGA del Parlamento Europeo es

[36] Carta firmada por 6 eurodiputados del grupo Renew, 11 de mayo de 2022, otra por 16 investigadores internacionales, el 20 de mayo y la última firmada por más de 100 profesores e investigadores el 5 de julio de 2022.

[37] La carta denigratoria fue enviada al menos a Euractiv, Politico y The Guardian. Acusaba a Gregorio Martín y José Javier Olivas Osuna de promocionar teorías conspirativas y hacer falsas denuncias sobre los investigadores.

[38] Parlament.cat. Comissió d'Investigació sobre l'Espionatge de Representants Polítics, Activistes, Periodistes i llurs Familiars per part del Regne d'Espanya amb els Programes Pegasus i Candiru

la europarlamentaria de ERC Diana Riba, que no solo aparecía como presunta víctima, sino que tenía interés en demostrar espionaje ilegal a ella y los abogados de su pareja, Raül Romeva, uno de los líderes independentistas condenados. Se puede observar que muchos de expertos invitados en estas comisiones son colaboradores de Citizen Lab o de organizaciones cercanas como Amnistía, *Access Now* o *Electronic Frontier Foundation* (EFF).[39] En una tercera comisión sobre ciber-espionaje, ésta en el Consejo de Europa, tiene un papel central la representante de ERC Laura Castell[40]. Los informes de estas dos organizaciones supranacionales basan sus conclusiones casi exclusivamente en el informe de Citizen Lab y en la interpretación que de ellos hace la prensa independentista catalana[41]. Estos son muy críticos con España que sugieren espionaje ilícito y por motivos políticos, y omiten toda la evidencia empírica que apunta a graves problemas metodológicos del informe del laboratorio canadiense[42] y al hecho de que muchas de las presuntas víctimas están siendo investigadas por mandato judicial.

Además del impacto reputacional, esta campaña también puede tener importantes repercusiones legales e institucionales. Un ejemplo es el cese y posterior investigación de la directora del CNI Paz Esteban que se basa en la evidencia circunstancial aportada por Citizen Lab y en un peritaje contratado por las presuntas víctimas del Catalangate[43] sin que haya habido ningún análisis independiente de los teléfonos de estas. Es importante recordar que hay diez causas judiciales basadas en los resultados del informe CatalanGate

(CIERPAPFRE) https://www.parlament.cat/web/composicio/comissions/informacio-comissio/index.html?p_legislatura=13&p_tipus=COM&p_codi=1239

[39] European Parliament, eMeeting for Committees. PEGA. https://emeeting.europarl.europa.eu/emeeting/committee/en/archives/PEGA

[40] ERC. Nota de Premsa. 8 de septiembre de 2023. Esquerra Republicana contribueix en el primer informe del Consell d'Europa que carrega contra l'Estat per l'ús de Pegasus.

[41] VozPopuli. El informe europeo del espionaje de Pegasus se basa en 'El Nacional.cat' y el estudio del Citizen Lab. 9 de noviembre de 2022. https://www.vozpopuli.com/internacional/informe-europeo-espionaje-pegasus.html

[42] European Parliament. PEGA. 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. 23 may 2023. https://www.europarl.europa.eu/committees/en/pega/documents/latest-documents ; Parliamentary Assembly. Council of Europe. Five member states must investigate spyware abuse, says PACE. 11 de octubre de 2023. https://pace.coe.int/en/news/9243/five-member-states-must-investigate-spyware-abuse-says-pace

[43] VozPopuli. El perito que avaló la imputación de la exjefa del CNI trabajó para la Generalitat en el Catalangate. https://www.vozpopuli.com/espana/catalangate-perito-imputacion-directora-cni-generalitat.html. José Navarro lleva tiempo trabajando para los líderes independentistas, no está colegiado como Profesional de Ingenieros Técnicos en Informática, ni tiene diploma superior en informática. El Triangle. El perito que ha contratado Pere Aragonès en el caso Pegasus, acusado de intrusismo profesional. 3 noviembre 2023. https://www.eltriangle.eu/es/2023/11/03/el-perito-que-ha-contratado-a-pere-aragones-en-el-caso-pegasus-acusado-de-intrusismo-profesional/

en España y varias otras en juzgados de otros países[44] y que tres de los abogados de los líderes independentistas condenados en 2019 Gonzalo Boye, Andreu Van den Eynde y Jaume Alonso-Cuevillas están en la lista de presuntas víctimas de espionaje y han declarado que este hecho podría servir para anular las condenas a sus defendidos (Olivas Osuna 2022, 137-139). El diputado independentista Albert Botran, y presunta víctima de Pegasus, fue elegido como integrante de la Comisión de Secretos del Parlamento tras la publicación del informe de Citizen Lab que en teoría fiscaliza la acción de los servicios de inteligencia[45].

También se puede apreciar la relevancia del caso a nivel de ciberseguridad. Citizen Lab y Amnistía Internacional actúan coordinadamente y se presentan a sí mismas como las únicas organizaciones capaces de detectar ataques con Pegasus y otros *spyware*. Se apoyan en un conjunto de organizaciones con las que colaboran muy estrechamente, como EFF, *Digital Rights Foundation*, *Access Now*, R3D, *Red Line for Gulf*, *Article 19* y *Threat Intel Coalition*, y en un nutrido grupo de periodistas y activistas que las promocionan públicamente sus trabajos y quienes ignoran o descalifican cualquier crítica que se vierta contra esta red (Grupo *Forbidden Stories*, Edward Snowden, Glenn Greenwald, Marc Owen Jones y David Kaye entre otros), como ha sucedido en el caso de CatalanGate. El comportamiento cartelístico de esta red dificulta que surjan nuevos actores en este sector que puedan corroborar o cuestionar sus métodos y conclusiones o puedan actuar como peritos independientes.

5. CONCLUSIONES

Este capítulo ha mostrado la complejidad y la variedad de agentes e instituciones que pueden instrumentalizarse en una campaña de desinformación, en este caso la del CatalanGate. La falta de transparencia metodológica, ocultación de conflictos de intereses y el lenguaje y forma en que se presentan los resultados en esta investigación pueden ser

[44] VozPopuli. Catalangate: una decena de causas del espionaje depende de si Sánchez desclasifica los informes del CNI. 18 de octubre de 2023. https://www.vozpopuli.com/espana/causas-espionaje-catalan-pegasus-gobierno-desclasifica-informes-cni.html. El Independiente. El mapa de las querellas independentistas por Pegasus abarca seis países. 8 de mayo de 2022. https://www.elindependiente.com/espana/2022/05/08/el-mapa-de-las-querellas-independentistas-por-pegasus-abarca-seis-paises/

[45] La Vanguardia. Rufián, Nogueras y Botran formarán parte de la comisión de secretos oficiales. 28 abril de 2022 https://www.lavanguardia.com/politica/20220428/8229947/rufian-nogueras-botran-formaran-parte-comision-secretos-oficiales.html

considerados una maniobra para manipular a la audiencia. El que una investigación haya sido financiada por unas multinacionales interesadas en encontrar infecciones para una demanda judicial y que el trabajo de campo fuese realizado por las propias presuntas víctimas quienes tenían interés en maximizar el número de casos por motivos políticos, son hechos muy relevantes y que contravienen las convenciones científicas y los mismos reglamentos de la Universidad de Toronto[46].

El CatalanGate sirve para ilustrar también el problema de seguridad, originalmente planteado por Platón en su *República ¿Quis custodiet ipsos custodes?*, es decir ¿Quién vigilará a los vigilantes? Las sociedades democráticas necesitan servicios de inteligencia capaces de detectar amenazas terroristas, conspiraciones contra el orden democrático y grupos de crimen organizado. Pero cómo asegurarse que estos organismos de vigilancia operen dentro de la ley y trabajen para los intereses colectivos del país, y no para intereses partidistas o personales.

Para garantizar el comportamiento ejemplar de estas agencias de vigilancia tradicionalmente se crea regulación específica y mecanismos de control, como son las comisiones parlamentarias de secretos y de investigación. También se ha confiado en organizaciones de la sociedad civil para actuar como guardianes de los derechos y libertades. Citizen Lab y Amnistía Internacional son ejemplos de ello. Éstas se suponía que fiscalizaban no sólo a los gobiernos, sino también a las grandes corporaciones tecnológicas que, como Facebook, Google o Apple, han estado envueltas en escándalos relacionados con la desinformación y la violación del derecho a privacidad.

Pero ¿qué hacer si las organizaciones a las que se confía la vigilancia para evitar abusos relativos a nuestra privacidad están instrumentalizadas políticamente o trabajan para quienes supuestamente deberían estar controlando? Como este caso, para grandes corporaciones tecnológicos o grupos que amenazan la seguridad y estabilidad en un país La rendición de cuentas es fundamental, y se espera que los gobiernos y grandes compañías actúen con un nivel adecuado de transparencia. También deben aplicarse reglas similares de rendición de cuentas y transparencia a los presuntos guardianes, en este caso a quienes estudian los casos de ataques de spyware.

---

[46] University of Toronto. Research Integrity. https://research.utoronto.ca/research-integrity/research-integrity ; University of Toronto Governing Council. Policy on Ethical Conduct in Research, https://governingcouncil.utoronto.ca/system/files/import-files/ppmar281991i4820.pdf

Desgraciadamente, Citizen Lab ha demostrado una total falta de transparencia. Esta opacidad afecta no sólo a los datos sobre la financiación del centro canadiense e indicios de ataques y supuestas infecciones de teléfonos de los políticos independentistas, sino también a información sobre cuándo, cómo, dónde y quién realizó los análisis forenses, la cadena de custodia de las pruebas y la documentación de los procesos. El prestigio personal de los investigadores, por sí sólo, no debe considerarse un substituto de validaciones externas. Citizen Lab es un actor muy influyente en el ámbito de la ciberseguridad. Sus informes se utilizan en investigaciones parlamentarias y judiciales y sus conclusiones publicadas en los grandes medios de comunicación internacionales.

A pesar de los evidentes problemas metodológicos y sesgo, y del rechazo frontal a responder a las críticas y rendir cuentas de Citizen Lab este informe ha tenido un enorme impacto político y mediático. En definitiva, el caso CatalanGate demuestra la vulnerabilidad del medios e instituciones políticas ante campañas de desinformación y manipulación y sugiere la necesidad de continuar investigando las sinergias entre los mundos académico, políticos y empresarial en lo relativo a la generación y diseminación de información engañosa.

1.1. Bibliografía

Alherbawi, N., Shukur, Z., & Sulaiman, R. (2013). Systematic literature review on data carving in digital forensic. *Procedia Technology, 11*, 86-92.

Ayers, R., Brothers, S. & Jansen, W. (2014). Guidelines on Mobile Device Forensics. NIST Special Publication 800-101. http://dx.doi.org/10.6028/NIST.SP.800-101r1

Barberà, O. (2021). 14 All fake? Information disorders and the 2017 referendum in Catalonia. In S. Baume, V. Boillet, V. Martenet (eds.) *Misinformation in Referenda*. Routledge: London.

Bago, B., Rand, D. G., & Pennycook, G. (2020). Fake news, fast and slow: Deliberation reduces belief in false (but not true) news headlines. *Journal of Experimental Psychology: General, 149*(8), 1608–1613.

Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. Oxford University Press.

Besley, T., & Robinson, J. A. (2010). Quis custodiet ipsos custodes? Civilian control over the military. *Journal of the European Economic Association*, *8*(2-3), 655-663.

Brown, N. I. (2020). Deepfakes and the Weaponization of Disinformation. *Virginia Journal of Law & Technology*, *23*, 1-59.

Citizen Lab (2023). Publications. Research Reports. https://citizenlab.ca/publications/

Curiel, C. P., Rúas-Araújo, X., & Barrientos-Báez, A. (2022). Misinformation and Fact-checking on the disturbances of the Procés of Catalonia. Digital impact on Public and Media. *KOME: An International Journal of Pure Communication Inquiry,* https://dx.doi.org/10.17646/KOME.75672.88

Di Domenico, G., Sit, J., Ishizaka, A., & Nunan, D. (2021). Fake news, social media and marketing: A systematic review. *Journal of Business Research*, *124*, 329-341.

Douglas, K. M., Uscinski, J. E., Sutton, R. M., Cichocka, A., Nefes, T., Ang, C. S., & Deravi, F. (2019). Understanding conspiracy theories. *Political Psychology*, *40*, 3-35.

ENISA (2013) Digital forensics: Handbook, Document for teachers, European Union, September 2012, https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/digital-forensics-handbook

European Commission (2018) Fake news and online disinformation. *Digital Single Market-Policy*. https://ec.europa.eu/digital-single-market/en/fake-news-disinformation

Eysenbach, G. (2009). Infodemiology and Infoveillance: Framework for an Emerging set of Public Health Informatics Methods to Analyze Search, Communication and Publication Behavior on the Internet. *Journal of Medical Internet Research*, *11*(1), e1157. 10.2196/jmir.1157

Fernández-Roldán, A., Elías, C., Santiago-Caballero, C. & Teira, D. (2023). Can we detect bias in political fact-checking? Evidence from a Spanish case study, *Journalism and Practice*

Fetzer, J. H. (2004). Disinformation: The use of false information. *Minds and Machines*, 14, 231-240.

Gallotti, R., Valle, F., Castaldo, N., Sacco, P., & De Domenico, M. (2020). Assessing the risks of 'infodemics' in response to COVID-19 epidemics. *Nature Human Behaviour*, *4*(12), 1285-1293.

Graves, L., & Anderson, C. W. (2020). Discipline and promote: Building infrastructure and managing algorithms in a "structured journalism" project by professional fact-checking groups. *New Media & Society*, *22*(2), 342-360.

Gwebu, K. L., Wang, J., & Zifla, E. (2022). Can warnings curb the spread of fake news? The interplay between warning, trust and confirmation bias. *Behaviour & Information Technology*, *41*(16), 3552-3573.

House of Commons (2018). Disinformation and "fake news": Interim report, fifth report of session 2017-2019. *Digital, Culture, Media and Sport Committee. UK Parliament*, HC363, 24 Julio 2018. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf

Keen, B. (1969). The black legend revisited: assumptions and realities. *Hispanic American Historical Review*, *49*(4), 703-719.

Krafft, P. M., & Donovan, J. (2020). Disinformation by design: The use of evidence collages and platform filtering in a media manipulation campaign. *Political Communication, 37*(2), 194-214.

Krishnan, S., Zhou, B., An, MK (2019). Smartphone Forensic Challenges. *International Journal of Computer Science and Security 13 (5), 183 - 200;*

Kruglanski, A. W., Molinario, E., Ellenberg, M., & Di Cicco, G. (2022). Terrorism and conspiracy theories: A view from the 3N model of radicalization. *Current Opinion in Pychology*, *47*, 101396.

Llorca-Asensi, E., Sánchez Díaz, A., Fabregat-Cabrera, M. E., & Ruiz-Callado, R. (2021). "Why Can't We?" Disinformation and Right to Self-Determination. The Catalan Conflict on Twitter. *Social Sciences*, *10*(10), 383.

Moffitt, B. (2015). How to perform crisis: A model for understanding the key role of crisis in contemporary populism. *Government and Opposition*, 50(2), 189-217

España Global (2019). *La realidad sobre el proceso independentista*. Ministerio de Asuntos Exteriores y Cooperación de España. https://www.exteriores.gob.es/Embajadas/paris/es/Comunicacion/Noticias/Paginas/Articulos/20191010_NOT1.aspx

McKay, S., & Tenove, C. (2021). Disinformation as a threat to deliberative democracy. *Political Research Quarterly*, *74*(3), 703-717.

Miller, B. M. (2021). Did Fake News Unite the Home Front behind a War with Spain? A Reconsideration of US Press Coverage, 1895–1898. *Home Front Studies*, *1*(1), 1-31.

OECD (2023) The OECD DIS/MIS Resource Hub Joining forces to fight dis- and misinformation. *Organisation for Economic Co-operation and Development*. https://www.oecd.org/stories/dis-misinformation-hub/

Olivas Osuna, J. J. (2021). From chasing populists to deconstructing populism: A new multidimensional approach to understanding and comparing populism. *European Journal of Political Research*, *60*(4), 829-853.

Olivas Osuna, J.J. (2022). The Pegasus spyware scandal: a critical review of Citizen Lab's "CatalanGate". European Parliament. Renew Group. Bruselas. https://eprints.lse.ac.uk/118492/

Olivas Osuna, J. J., & Rama, J. (2021). COVID-19: a political virus? VOX's populist discourse in times of crisis. *Frontiers in Political Science, 3*, 57, https://www.frontiersin.org/articles/10.3389/fpos.2021.678526/full

Posetti, J., & Matthews, A. (2018). A short guide to the history of 'fake news' and disinformation. *International Center for Journalists*, *7*(2018), 2018-07.

Serrano-Puche, J. (2021). Digital disinformation and emotions: exploring the social risks of affective polarization. *International Review of Sociology*, *31*(2), 231-245.

Scott-Railton, J., Campo, E., Marczak, B., Razzak, B. A., Anstis, S., Böcü, G., Solimano, S. & Deibert, R. (2022). Catalangate: Extensive mercenary spyware operation against Catalans using pegasus and Candiru. *The Citizen Lab. Munk School, University of Toronto,* https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

UN (2022). Countering disinformation for the promotion and protection of human rights and fundamental freedoms. Report of the Secretary General. *United Nations General Assembly*. https://www.un.org/en/countering-disinformation

UN (2022b). Berkeley Protocol on Digital Open Source Investigations. New York. Human Rights Center, UC Berkeley School of Law and United Nations Human Rights Office of the High Commissioner. https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf

UNIDIR (2018). The Weaponization of Increasingly Autonomous Technologies: Artificial Intelligence. *United Nations Institute for Disarmament Research.* https://www.unidir.org/publication/weaponization-increasingly-autonomous-technologies-artificial-intelligence .

Voo, J., Hermani, I. & Cassidy, D. (2022). National Cyber Power Index 2022. *Belfer Center for Science and International Affairs, Harvard Kennedy School*. https://www.belfercenter.org/publication/national-cyber-power-index-2022