ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/369186524

# El Caso Pegasus: Una revisión crítica del informe "CatalanGate" de Citizen Lab

**Technical Report** · March 2023

CITATIONS
0

READ
1

**1 author:**

Jose Javier Olivas Osuna
National Distance Education University
**81** PUBLICATIONS **249** CITATIONS

SEE PROFILE

**Some of the authors of this publication are also working on these related projects:**



Comparing media reporting of the Indignados and Aganaktismenoi movements in Spain, Greece and Germany View project



Debating Brexit impact at local level: a mixed methods comparative study View project

All content following this page was uploaded by Jose Javier Olivas Osuna on 13 March 2023.

The user has requested enhancement of the downloaded file.

# El caso Pegasus
## Una revisión crítica del informe «CatalanGate» de Citizen Lab

*por José Javier Olivas Osuna, Departamento de Ciencias Políticas y de la Administración, Universidad Nacional de Educación a Distancia (UNED), Madrid*

# Índice

| | |
|---|---|
| **Prólogo** | 08 |
| **Resumen ejecutivo** | 14 |
| **Línea temporal** | 20 |
| **«CatalanGate»: un informe no validado de forma independiente** | 28 |
| **Falta de transparencia** | 40 |
| **Una confianza anormal en la fiabilidad de la metodología y rechazo de falsos positivos** | 56 |
| **¿Cuándo y dónde se realizaron los análisis forenses?** | 66 |
| **Conflicto de intereses y confiar el trabajo de campo a un activista político sin experiencia previa** | 74 |
| **El extraño origen y calendario de la investigación** | 90 |
| **Otras contradicciones en las que incurrieron los autores del informe** | 100 |
| **¿Un trabajo de campo condicionado por intereses económicos? Facilitando «munición» para los juicios** | 112 |
| **¿Una campaña de propaganda política?** | 122 |
| **¿Espionaje con Pegasus como herramienta para invalidar los juicios?** | 136 |
| **Conexiones con Rusia y estrategia de blockchain para la secesión** | 140 |
| **Reacción inusual de la Universidad de Toronto** | 178 |
| **Las «víctimas» de «espionaje ilegal»** | 192 |
| **Colaboradores de Citizen Lab intentan silenciar al autor del informe** | 208 |
| **Conclusiones** | 218 |
| **Agradecimientos** | 222 |
| **Sobre el autor** | 224 |
| **Bibliografía** | 228 |

# Prólogo

El 10 de marzo de 2022, el Parlamento Europeo decidió crear el Comité PEGA para investigar presuntas infracciones o mala administración en la aplicación de la legislación de la UE en relación con el uso de Pegasus y software de vigilancia (*spyware*) equivalente, después de hacerse público el Proyecto Pegasus, en el que a raíz de una investigación colaborativa en la que participaron más de 80 periodistas de 17 organizaciones de medios de comunicación de 10 países bajo la coordinación de Forbidden Stories, se denunciaba el uso masivo software espía Pegasus de NSO Group para facilitar la comisión de violaciones de derechos humanos a gran escala en todo el mundo.

El Comité PEGA ha recopilado, durante el transcurso de sus trabajos, información sobre las denuncias de que algunos Estados miembros o terceros países hubieran utilizando software de vigilancia intrusiva contra ciudadanos europeos, en la medida en que ello viola los derechos y libertades consagrados en la Carta de los Derechos Fundamentales de la UE. Durante su mandato el Comité ha realizado numerosas sesiones informativas y audiencias con responsables políticos, investigadores, expertos en ciberseguridad, periodistas y presuntas víctimas, con el objeto de presentar un informe final en el cual, además de relatar los hechos acaecidos, se propongan medidas concretas que garanticen los derechos y libertades de los ciudadanos europeos frente a intrusiones ilegales a su intimidad.

En el caso de España, las sospechas del uso de programas espía se centraban alrededor de dos grupos de posibles «víctimas». Por un lado, en un informe publicado por el diario The Guardian en mayo de 2022, se apuntaba a Marruecos como el posible autor del espionaje de más de 200 móviles españoles, entre los que destacaban los del presidente del gobierno de España, Pedro Sánchez; la ministra de Defensa, Margarita Robles; la entonces ministra de Exteriores, Arancha González Laya; y el ministro del Interior Fernando Grande-Marlaska.

Y por otro, el laboratorio CitizenLab publicó, en abril de 2022, un informe denominado «CatalanGate: Extensive mercenary spyware operation against Catalans using Pegasus and Candiru» en el que denunciaba el supuesto uso de estos programas espía para infectar los teléfonos de al menos 65 políticos, abogados y miembros de organizaciones del entorno separatista catalán.

Las diferentes reuniones de la Comisión habían desarrollado sus trabajos con normalidad, hasta la preparación de la sesión correspondiente a la audiencia parlamentaria sobre la participación de España en el escándalo del software espía Pegasus, programada para el martes 29 de noviembre de 2022. Tras una filtración del programa de la sesión prevista

para la audiencia, uno de los dos expertos españoles invitados a participar en la misma, fue excluido a última hora de la lista de ponentes después de que el entorno de Citizen Lab hiciera circular una carta entre eurodiputados desacreditando el trabajo de estos dos expertos. En dicha misiva, se aducía una supuesta falta de conocimiento técnico sobre espionaje y se les acusaba de haber promovido teorías de la conspiración y falsedades sobre otros investigadores, así como de participar en el acoso a presuntas víctimas de espionaje y expertos que habían investigado los casos. La carta que pedía el veto a los dos ponentes fue firmada entre otros por Ronald Deibert y John Scott-Railton, ambos autores del informe Catalangate. Tras recibir la carta, el lunes 21 de noviembre se celebró una reunión de los coordinadores del comité PEGA. En ella, el grupo Renew, del que formo parte y que a mi solicitud había propuesto a uno de ellos, el académico e investigador José Javier Olivas, retiró su nombre del programa.

Ante esta lamentable decisión e intolerables acusaciones, como eurodiputado de Ciudadanos envié una carta a los miembros de la comisión PEGA denunciando que esta grave decisión sentaba un precedente peligroso: demostraba que las presiones externas determinaban el desarrollo del trabajo de una institución democrática y decidían quien puede o no ser invitado a participar de los trabajos de una comisión parlamentaria. Una situación que enviaba un inquietante mensaje de falta de imparcialidad, pluralidad y contraste de argumentos e ideas. Si se aceptaban cancelaciones, censuras y vetos de quienes, por rigor académico y metodología, criticaban o cuestionaban las fuentes del informe, evidenciaría que el comité, sus trabajos y sus conclusiones podían ser manipulados e instrumentalizados para enterrar la verdad. Pero, desgraciadamente, el veto y la censura se impusieron.

Es por ello, y con la determinación de combatir la censura, los vetos y cancelaciones en la sede de la democracia europea, que publico esta revisión crítica del informe «CatalanGate» de Citizen Lab elaborado por el profesor, académico e investigador José Javier Olivas.

El Parlamento Europeo es la casa de la palabra, de la libertad de expresión y del pensamiento crítico. Valores sobre los que se ha construido la idea de Europa y que la definen.

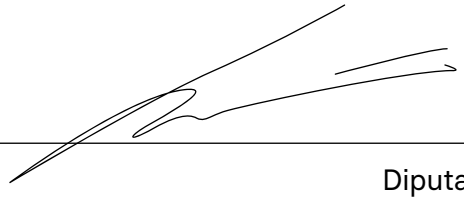
Pero el proyecto europeo, y sus valores democráticos, tienen poderosos adversarios externos, e internos. Y no solo están amenazados por aquellos que manifiestamente cuestionen la democracia liberal desde el populismo o el nacionalismo, sino también por aquellos que, con la intención de defenderla, renuncian a practicar los valores que la animan: el respeto a la libertad de opinión y al pensamiento crítico.

La defensa de estos dos principios frente a la violencia ejercida desde el poder, ha sido y es uno de las constantes que han marcado el agón histórico del pensamiento europeo: Hoy en día, ese libre pensamiento se enfrenta no tanto o no solo al poder político, como también al poder de un pensamiento único que desarrolla estrategias de cancelación en los medios de comunicación, en las redes sociales y también en instituciones académicas y democráticas. Un peligroso neo macartismo que va impregnando como un tóxico chapapote todo el debate público.

Lo fáctico no puede ni debe someterse a una conveniente interpretación manipuladora de presuntos hechos que solo busca reforzar o bien prejuicios o bien conclusiones predeterminadas. Una hipótesis no es una tesis, ni una teoría. La hipótesis es una proposición que se basa en el conocimiento existente y que sirve como punto de partida de una investigación. Una tesis es una afirmación que se presenta como una premisa que debe mantenerse o probarse. Y una teoría es una explicación probada y justificada mediante una serie de hechos comprobados y verificados. Una teoría siempre debe estar respaldada por evidencia, mientras que una hipótesis es apenas un posible resultado, que puede y debe ser comprobado y refutado. Que alguien pretenda pasar una hipótesis por una teoría, es peligroso y debe ser denunciado.

Camuflar sospechas, conjeturas o especulaciones como certezas, y que estas articulen un informe del parlamento europeo, despreciando, silenciando o directamente censurando a quienes cuestionan esas falsas evidencias desde argumentos críticos, es un ejercicio de deshonestidad política inaceptable. Como lo es confundir voluntariamente las suposiciones por hechos probados y caer en la difamación como argumento de autoridad para refutar cualquier análisis crítico que cuestione esa supuesta verdad. Pero lo que es especialmente grave es el atentado que ello supone a los valores y principios no solo del Parlamento Europeo, sino de la propia idea de Europa: el respeto a la libertad de opinión y la defensa del pensamiento crítico.

Que este estudio sirva para aportar argumentos al debate público y contribuya a fundamentar una opinión veraz sobre la cual poder tomar las decisiones adecuadas para defender los derechos y libertades de los ciudadanos europeos sin sacrificar nuestros valores y principios.



**Jordi Cañas Pérez**

Diputado del Parlamento Europeo
*Ciudadanos (Cs) - Renew Europe*

# Resumen ejecutivo

El presente documento disecciona el informe «CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru»,[1] publicado el 18 de abril de 2022 por Citizen Lab de la Escuela Munk de Asuntos Globales y Políticas Públicas, Universidad de Toronto, y revela una serie de graves problemas metodológicos y éticos que socavan gravemente su valor como base probatoria para las comisiones parlamentarias y los juicios judiciales. Este análisis crítico muestra que el diseño de la investigación de Citizen Lab, el trabajo de campo y la notificación de los resultados del informe «CatalanGate» contravienen las normas comúnmente aceptadas de conducta e integridad de la investigación académica. La variedad y gravedad de los escollos descubiertos sugieren que Citizen Lab y las organizaciones políticas que colaboraron con ellos en la elaboración del informe pueden haber intentado inducir deliberadamente un fuerte sesgo político para dar forma a la opinión pública y lograr un fuerte impacto mediático. Esta revisión crítica recomienda a la Universidad de Toronto que ponga en marcha una investigación independiente sobre este informe y que retracte su publicación. Resumen de algunos de los principales problemas detectados:

1) *La investigación CatalanGate infringe las directrices y principios básicos de criminalística digital, prescrita, entre otros, por la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y el Protocolo de Berkeley sobre investigaciones de código abierto digital de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OHCHR).*

*1/ John Scott-Railton, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, and Ron Deibert (2022). CatalanGate; Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru. Citizen Lab, 18 de abril de 2022*

2) *Los resultados comunicados en este estudio no son reproducibles y no han sido revisados o validados por pares de forma independiente.*

3) *Existe una falta muy inusual de transparencia en lo que respecta a las opciones metodológicas y de diseño de la investigación. Los autores se niegan a comunicar el número de dispositivos investigados o la proporción de positivos en el análisis. No se han notificado grupos de control ni intervalos de confianza de los análisis.*

4) *Los autores se niegan a informar de cuándo, dónde y por quién se realizaron los análisis forenses digitales. No hay pruebas de que Citizen Lab haya realizado ningún análisis confirmatorio en persona (sobre el terreno) para verificar las infecciones. No se hace referencia a ningún procedimiento para garantizar la cadena de custodia de pruebas, como se espera en un análisis forense digital serio.*

5) *Los datos sobre infecciones e intentos de infección de dispositivos se presentan agrupados, lo que puede inducir al lector a creer que todas las presuntas víctimas de la denuncia han sido espiadas.*

6) *Ronald Deibert, director de Citizen Lab, afirma una fiabilidad del 100 % de sus procesos analíticos y se niega a considerar la posibilidad de falsos positivos u otros errores; esto contrasta con la mayor parte de la literatura general sobre análisis forenses y ciencias sociales.*

7) *Es evidente que los participantes y algunos autores intentaron maximizar el número de positivos. La reticencia a presentar muestras para su validación externa y la notificación de intentos de infección junto con infecciones exitosas parecen confirmarlo.*

8) *Siguen sin divulgarse diversos conflictos de intereses (políticos y económicos), en los que participan los autores del informe y las personas que colaboran en su trabajo de campo.*

9) *El trabajo de campo fue coordinado por el Sr. Elies Campo, activista a favor de la independencia, y presunta víctima del espionaje sin experiencia previa en investigación y que carece de título de enseñanza superior. Este autor también hizo afirmaciones falsas sobre su situación laboral y no estuvo afiliado a Citizen Lab durante la mayor parte del período de investigación.*

10) *Apartentemente solo se analizaron los dispositivos de políticos y activistas partidarios de la independencia. Los autores no explican los criterios utilizados en el muestreo de «bola de nieve». Existen pruebas muy sólidas que sugieren que los casos sometidos a análisis fueron filtrados por partidos políticos.*

11) *La comunicación de los resultados de la investigación de CatalanGate refleja un fuerte sesgo político, sesgo de selección y falta de rigor. A menudo, la información se agrupa de manera problemática o se omite para inducir determinadas opiniones no neutras.*

12) *Según los principales participantes en el estudio, la investigación de Citizen Lab en España buscó pruebas para alimentar los procesos judiciales contra NSO por parte de WhatsApp, Apple y políticos secesionistas catalanes. El anuncio por parte de Apple de una contribución de 10 millones de dólares a los investigadores por su apoyo a la recogida de pruebas contra NSO y el nombramiento del director de Citizen Lab en la comisión que decide la asignación de la recompensa parecen sugerir intereses económicos no divulgados.*

13) *Los autores de Citizen Lab expresan acusaciones muy graves contra el Gobierno español por «espionaje ilegal» sobre la base de lo que el informe afirma ser «pruebas circunstanciales». El informe no aporta pruebas suficientes para sustentar estas acusaciones.*

14) *Mientras tanto, el informe no tiene en cuenta ninguna de las demás hipótesis alternativas plausibles. Resulta sorprendente que ni siquiera se mencione la posibilidad de vigilancia legalmente sancionada, falsos positivos o espionaje por parte de los servicios secretos de Rusia o países occidentales.*

15) *Existen muchas contradicciones y problemas éticos sobre cómo comenzó la investigación sobre el terreno en España en julio de 2020. En aquel momento, se inició una campaña de comunicación inusualmente potente, coordinada por partidos políticos secesionistas catalanes y una demanda en el plazo de una semana desde el primer análisis y antes de la confirmación de cualquier infección.*

16) *Durante la investigación, se advirtió a los participantes de que era probable que fueran espiados sin tener en cuenta que esta advertencia podía interferir en las investigaciones judiciales en curso. Muchos participantes estaban*

*siendo controlados legalmente por los servicios de seguridad españoles cuando se pusieron en contacto con ellos y explicaron cómo evitar la vigilancia. Otros estaban a la espera de juicio, y algunos incluso estaban cumpliendo penas de prisión.*

17) *El nombre CatalanGate se eligió para el informe publicado el 18 de abril de 2022 a fin de coincidir con el eslogan de la campaña de propaganda que los partidos y organizaciones secesionistas catalanes estaban preparando meses antes de la publicación del informe. La mayor organización secesionista registró el dominio «CatalanGate.cat» en enero de 2022. Además, desde 2012 se utiliza una cuenta de Twitter (182.600 seguidores) denominada actualmente «@catalangate» para promover diversas campañas de comunicación secesionistas.*

18) *Varios de los participantes en el estudio estaban en aquel momento y siguen siendo investigados por sus conocidos vínculos con los servicios de inteligencia rusos, la corrupción o la creación de Tsunami Democràtic, la plataforma ilegal basada en blockchain, destinada a derribar a las fuerzas de seguridad españolas y utilizada para coordinar disturbios violentos y bloqueos de carreteras, estaciones de tren y aeropuertos. La consideración como «víctimas» de varios líderes políticos y activistas investigados con autorización judicial por delitos graves (algunos de ellos condenados) parece arriesgada para un informe académico.*

19) *Sorprendentemente, en el informe se omiten completamente los vínculos bien documentados con Rusia y los intentos rusos de desestabilizar España y la UE apoyando a los secesionistas catalanes. La investigación de CatalanGate se inició precisamente en un momento en el que el apoyo al secesionismo catalán había disminuido a su nivel más bajo desde 2014, y cuando las conexiones con Rusia resultaron muy problemáticas con respecto a la opinión pública en relación con la invasión de Ucrania.*

20) *Los comunicados de prensa, las redes sociales y las declaraciones formales del Citizen Lab sobre el informe CatalanGate contienen numerosas contradicciones y declaraciones falsas. Los testimonios de varios participantes en la investigación contradicen el relato de Citizen Lab.*

21) *Dada la abundancia de problemas detectados, más de un centenar de investigadores de diversas universidades y disciplinas han solicitado a la Universidad de Toronto que abra una investigación independiente sobre*

*la realización de investigaciones de Citizen Lab durante la investigación CatalanGate (en dos cartas diferentes). Hasta la fecha, la Universidad de Toronto se ha negado a revisar el caso y ha ignorado muchas de las preguntas y peticiones de varios académicos y periodistas. También se ha negado a dar nombres de las organizaciones o individuos que financian Citizen Lab.*

22) *En lugar de modificar o retractar su informe, miembros del Citizen Lab, con la ayuda de algunos colaboradores externos, han llevado a cabo una campaña de difamación contra el autor de este informe y otros investigadores que han expresado críticas públicas a su informe CatalanGate. Esta campaña para silenciar las acusaciones de mala conducta en la investigación se llevó a cabo inicialmente en las redes sociales, pero ha llegado a la prensa internacional e incluso al Parlamento Europeo.*

En resumen, el informe CatalanGate no puede considerarse un trabajo académico riguroso. Infringe la mayoría de las convenciones académicas de investigación y no respeta los protocolos y principios de la investigación forense digital. Parece que se ha diseñado y llevado a cabo con el fin de afianzar un instrumento político para los nacionalistas catalanes, aportar pruebas de que tanto Apple como los partidos secesionistas estaban planificando, y tratando de justificar a posteriori la nulidad de juicios celebrados tras el intento unilateral de secesión en octubre de 2017, sobre la base de la supuesta vigilancia ilegal de abogados por parte de las autoridades españolas en el momento en que se celebraron estos juicios. Como tal, podría considerarse un elemento clave de una campaña de desinformación.

Queda fuera del alcance de esta revisión evaluar si en España se espió — legal o ilegalmente— a algunos de los participantes en la investigación o si Pegasus era el programa espía elegido. Lo que este análisis muestra es que el informe CatalanGate no cumple los requisitos mínimos para ser utilizado como base probatoria para los procedimientos jurídicos ni para las comisiones parlamentarias de investigación. En casos tan graves como el presente, se espera una investigación independiente por mala conducta en la investigación. Cualquier comisión parlamentaria o tribunal de justicia que investigue el CatalanGate debe solicitar expertos independientes — sin conexión con Citizen Lab o Amnesty Tech— para reproducir los análisis y evaluar su validez y fiabilidad. Es importante descartar los falsos positivos, así como identificar cualquier posible alteración o fabricación de pruebas, como los resultados positivos fabricados, aprovechando la ausencia de una cadena de custodia de pruebas en esta investigación.

La falta de controles de las acciones de guardianes de la seguridad y la privacidad online, como Citizen Lab, y su posible «captura» por parte de los grandes grupos tecnológicos y los grupos políticos partidistas deberían ser motivo de preocupación para la Unión Europea. Citizen Lab está en lo cierto al pedir la rendición de cuentas pública y transparencia a los Estados miembros europeos, pero también es importante que Citizen Lab se adhiera a estos mismos principios y que las acusaciones contra los gobiernos no alejen la atención de las responsabilidades y los desafíos a los que se enfrentan las grandes empresas tecnológicas en relación con la seguridad de internet.

# 1

# Línea temporal

## 2017

**01 de octubre**
Referéndum ilegal de independencia.

**26 de octubre**
Los emisarios del Kremlin se reúnen con el presidente de la Generalitat, Sr. Puigdemont, y ofrecen apoyo financiero y militar a una Cataluña independiente, a condición de redactar una legislación que favorezca las criptomonedas.

**27 de octubre**
El Sr. Puigdemont declara la independencia unilateral de Cataluña, pero suspende inmediatamente esta declaración.

**03 de noviembre**
El Tribunal español emite una orden de registro y detención internacional de 10 líderes proindependencia que huyeron de España. La mayoría de ellos aparecen más tarde como «víctimas de programas espía» en el informe CatalanGate.

## 2019

**10 de febrero**
Los líderes nacionalistas catalanes difunden un artículo de Komosomolskaya Pravda en el que se solicita la mediación de Rusia en el conflicto catalán.

**02 de setiembre**
El Tsunami Democràtic aparece en las redes sociales. Su mensaje es compartido por la mayoría de los líderes secesionistas y muchos de los participantes en la investigación CatalanGate.

**14 de octubre**
El Tribunal Supremo español anuncia penas de prisión para algunos dirigentes catalanes acusados de sedición, desobediencia y malversación. La plataforma Tsunami Democràtic pide la movilización en docenas de lugares y el bloqueo del aeropuerto de El Prat. Más de 100 vuelos se vieron afectados. Muchas de las movilizaciones acaban provocando disturbios violentos.

**18 de octubre**

Un tribunal español ordena el cierre de todas las páginas web vinculadas al Tsunami Democràtic y el ministro del Interior confirma que hay una investigación policial sobre sus organizadores. Entre el 14 de octubre y el 20 de octubre se documentaron más de 500 episodios violentos.

**29 de octubre**

WhatsApp presenta una demanda contra el grupo NSO sobre la base de las pruebas recogidas por Citizen Lab sobre los presuntos ataques con el *spyware* Pegasus.

**9 de noviembre**

El Tsunami Democràtic coordina muchos actos de desobediencia civil en toda Cataluña.

**11 de noviembre**

El Tsunami Democràtic pide a los activistas que bloqueen la autopista que conecta La Junquera con Francia. Primera acción coordinada con la aplicación móvil basada en blockchain.

**17 de diciembre**

Entrevista de Russia Today con Carles Puigdemont se emite en la televisión pública española pirateada, Canal 24 Horas. Se consideraque los responsables son hackers rusos.

**2020**

**8 de julio**

Sobre la base de la información filtrada, los periodistas Joaquín Gil (El País), Stefanie Kirchgaessner y Sam Jones (The Guardian) informan al Sr. Torrent de que ha sido víctima del ataque de Pegasus y le piden que se ponga en contacto con Citizen Lab.

**10 de julio**

El Sr. Torrent visita al Sr. Junqueras en prisión y a Citizen Lab se le autoriza a analizar los teléfonos de Esquerra Republicana de Catalunya (ERC). John Scott-Railton comienza a supervisar el teléfono del Sr. Torrent a distancia, buscando una posible infección desde Toronto, vía VPN.

**11 de julio**

Citizen Lab envía una nota al Sr. Torrent en la que afirma que figuraba en la lista de WhatsApp de posibles víctimas de los ataques de Pegasus durante la violación de seguridad de 2019.

**12 de julio**

Los Sres. Gil y Jones entrevistan al Sr. Torrent.

---

**14 de julio**

The Guardian y El País publican una exclusiva sobre el ataque Pegasus contra Roger Torrent y otros líderes separatistas. Los partidos nacionalistas y de izquierda solicitan una investigación parlamentaria sobre el espionaje de Pegasus.

---

**15 de julio**

En una reunión extraordinaria del grupo parlamentario ERC se debate la estrategia de comunicación sobre el supuesto caso de espionaje, y el Sr. Maragall insiste en utilizar el término «CatalanGate».

---

**16 de julio**

El Sr. Torrent anuncia en la radio Cadena SER que él y el Sr. Maragall están presentando una demanda contra el antiguo director del CNI. Posteriormente, Citizen Lab comunica al Sr. Torrent que el resultado del análisis forense remoto muestra que su teléfono no estaba infectado. Posteriormente, ERC escribe al Consejo de Europa, Amnistía Internacional y a un Relator Especial de las Naciones Unidas para pedir su apoyo para denunciar a España.

---

**17 de julio**

El Sr. Scott-Railton pone en contacto a políticos de ERC con el abogado mexicano Luis Fernando García para que este último preste asistencia para denunciar el espionaje en los medios de comunicación y en los tribunales.

---

**18 de julio**

Según el Sr. Torrent, el Sr. Scott-Railton dice a los políticos de ERC que «Tu asunto (el de Torrent) es la oportunidad de abrir un caso en la Unión Europea».

---

**21 de julio**

Oriol Sagrera explica al Sr. Torrent que Citizen Lab está interesado en suministrar «munición» a WhatsApp, Apple y partes independientes para presentar demandas.

| | | |
|---|---|---|
| | **27 de julio** | Citizen Lab confirma a ERC que ninguno de los teléfonos que habían enviado para su análisis estaba infectado. |
| | **28 de julio** | WhatsApp confirma que el Sr. Torrent figuraba en la lista de presuntas víctimas de ataques de Pegasus, pero que no puede confirmarse ninguna infección, ya que no se ha llevado a cabo un análisis forense exhaustivo. |
| | **31 de julio** | La encuesta del Centre d'Estudis d'Opinió (CEO) de la Generalitat confirma que el apoyo a la independencia ha disminuido hasta su nivel más bajo desde 2017 |
| | **21 de octubre** | Amnisitía Internacional escribe al Gobierno Español para pedir una investigación sobre el espionaje con Pegasus. |
| | **28 de octubre** | Las fuerzas policiales españolas detienen a 21 activistas secesionistas sospechosos de malversación relacionada con la financiación de la plataforma ilegal Tsunami Democràtic. |
| | **1 de noviembre** | La prensa española comienza a publicar audios grabados por la policía y otra información que demuestra los vínculos entre el movimiento separatista y Rusia, así como las actividades ilegales relativas a la organización y financiación de Tsunami Democràtic. |
| **2021** | **3 de setiembre** | El New York Times vincula la campaña separatista de Tsunami Democràtic con Rusia. The Guardian, Politico, The Times y otros medios de comunicación internacionales publican historias similares en las semanas siguientes. |
| | **23 de noviembre** | Apple anuncia que está preparando una demanda contra NSO y se compromete con una recompensa de 10 millones de dólares a Citizen Lab, Amnistía Internacional y otras organizaciones por recopilar pruebas para dicha demanda. |

## 2022

**10 de enero**

Organización secesionista Assemblea Nacional Catalana (ANC) registra el dominio «CatalanGate.cat», que actualmente es propiedad de la organización separatista Òmnium Cultural.

**1 de febrero**

Citizen Lab contrata a Elies Campo como *fellow* para ayudar a identificar a posibles víctimas.

**9 de marzo**

El Parlamento Europeo apoya por mayoría que se investiguen los vínculos entre Rusia y el movimiento secesionista catalán.

**17 de marzo**

La encuesta del CEO de Cataluña muestra que el apoyo al separatismo se encuentra en su nivel más bajo desde 2014.

**7 de abril**

El Parlamento catalán debate y rechaza la propuesta de condenar los contactos entre el Sr. Puigdemont y su entorno con Rusia.

**18 de abril**

Citizen Lab publica el informe «CatalanGate». El New Yorker publica el artículo de Ronan Farrow titulado «How democracies spy on their citizens», que hace referencia a España.

**21 de abril**

La editorial de Washington Post afirma que España parece haber cometido violaciones flagrantes de las libertades civiles en Cataluña y merece condena.

**11 de mayo**

Eurodiputados al Parlamento Europeo (PE) del grupo Renew Europe envían una carta a la Universidad de Toronto solicitando algunas respuestas sobre hechos inusuales en torno a la investigación

**13 de mayo**

El Sr. Deibert responde a las preguntas en un documento formal enviado al Sr. Jordi Cañas, primer signatario de la carta de los diputados al PE del Grupo Renew.

| | |
|---|---|
| **20 de mayo** | Dieciséis profesores e investigadores presentan una carta solicitando a la Universidad de Toronto que inicie una investigación independiente sobre el informe CatalanGate. |
| **5 de julio** | Más de 100 profesores e intelectuales independientes piden a la Universidad de Toronto que inicie una investigación independiente sobre el informe CatalanGate. |
| **19 de julio** | La Universidad de Toronto rechaza formalmente todas las solicitudes de apertura de una investigación. |
| **22 de julio** | Se solicita una investigación al *Ombudsperson* de la Universidad de Toronto en relación con el informe CatalanGate. Se presenta una solicitud para activar la Ley de Libertad de Información y Protección de la Privacidad (FIPPA) en la que se pide información sobre Citizen Lab y sus conexiones con agentes políticos catalanes, WhatsApp y Apple. |
| **2 de agosto** | El *Ombudsman* de la Universidad de Toronto se niega a investigar el caso. |
| **21 de setiembre** | La Oficina de Libertad de Información y Protección de la Privacidad revela información relativa al Citizen Lab, pero retiene gran parte de la información solicitada, como el nombre de las instituciones de financiación y más de 112 páginas de acuerdos y actas solicitadas. |
| **6 de octubre** | Antoni Comín, Diana Riba y Jordi Solé testifican como presuntas víctimas de Pegasus en la Comisión de Investigación PEGA del Parlamento Europeo. |
| **22 de diciembre** | El Citizen Lab admite que el Sr. Antoni Comín no fue víctima de espionaje, sino que se le atribuyó erróneamente la infección de un teléfono perteneciente a otro participante. |

# 2

# «CatalanGate»: un informe no validado de forma independiente

Las conclusiones de Citizen Lab han suscitado una enorme atención por parte de los medios de comunicación, dada lagravedad de las acusaciones contra el Gobierno español. Como explicará esta revisión crítica, no solo la prensa española, sino también la internacional, recogió la historia, dando por sentada la fiabilidad de las pruebas que Citizen Lab había revelado.

Desafortunadamente, los datos sobre presuntas infecciones por programas espía y ataques a políticos y activistas del separatismo catalán no se pusieron a disposición de analistas externos: estos se basaban solo en la reputación del centro de investigación canadiense para evaluar la idoneidad de las acusaciones contra España. La falta de rendición de cuentas pública mostrada por un actor muy influyente en el ámbito de la ciberseguridad, cuya labor se utiliza como base probatoria en muchas investigaciones parlamentarias y judiciales, es muy problemática.

El informe «CatalanGate» no fue objeto de revisión *inter pares* ni validado por expertos independientes. Citizen Lab compartió cuatro muestras a Amnesty Tech. Sin embargo, no se explica claramente por qué solo cuatro muestras (Jordi Sànchez, Sonia Urpí, Elisenda Paluzie y Meritxell Bonet) fueron sometidas a una validación externa o por qué Citizen Lab no eligió una organización independiente para dicha revisión. Hay 27 presuntas víctimas de ataques sobre las que Citizen Lab no pudo determinar ninguna fecha (o intervalo de tiempo) de infección (o decidió no informar al respecto). No parece lógico que ninguno de estos casos «más difíciles» se haya sometido a prueba de posibles falsos positivos.[2]

El Sr. Ronald Deibert,[3] director de Citizen Lab y coautor del informe, afirma que las conclusiones del informe son teóricamente reproducibles, pero que los expertos independientes no pueden reproducir esta investigación específica, ya que requeriría el consentimiento de los participantes a la investigación.[4] Es destacable la reticencia a poner muestras a disposición de expertos independientes en un caso en el que las presuntas víctimas se han manifestado voluntaria y públicamente para que se examinen sus dispositivos. De todos modos, deberían haber obtenido la autorización expresa de cuatro de las presuntas víctimas, el Sr. Jordi Sànchez, la Sra. Sonia Urpí, la Sra. Elisenda Paluzie y la Sra.

2/ *Además, el Sr. Sànchez y la Sra. Paluzie fueron supervisados por los servicios secretos españoles tras un mandato judicial. La Vanguardia. Los 18 espiados por el CNI. 14 de mayo de 2022* https://www.lavanguardia.com/politica/20220514/8266136/18-espiados-cni-pegasus.html

3/ *Obsérvese que en el presente informe el Sr. y la Sra. se utilizan en vez de Dr. o Prof (como correspondería a Ronald Deibert y otros)*

4/ *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 la Sra. Lorraine Ferris al Sr. 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 *Página 3*

Meritxell Bonet, cuyos teléfonos fueron examinados por Amnesty Tech.[5] Además, como el Sr. Deibert explica en esa misma carta, Citizen Lab ya había compartido muestras de infección en otras investigaciones con Microsoft, Apple, Lookout Security y Project Zero en Google.

Hasta la fecha, los teléfonos de al menos 7 de las presuntas víctimas han sido solicitados ante los tribunales como parte de las denuncias formales que lanzaron contra el fabricante de Pegasus, el Grupo NSO. Sin embargo, ninguno de ellos ha proporcionado los teléfonos supuestamente atacados para que se verifiquen las infecciones por parte de expertos técnicos independientes designados por los tribunales.[6] ¿Por qué son tan reacios a que se reexaminen sus dispositivos?

Otra decisión de investigación poco ortodoxa de Citizen Lab es la de emplear a Amnesty Tech para una «validación independiente»[7]. Los dos expertos de Amnesty Tech en el ámbito de la criminalística digital son Claudio Guarnieri y Etienne Maynier, ambos colaboradores en Citizen Lab y creadores de la herramienta móvil de verificación (MVT) utilizada para realizar análisis forenses de dispositivos móviles con el fin de encontrar signos de posible compromiso.[8] Casualmente, Citizen Lab publicó una «revisión *inter pares* independiente» de esta metodología (que es utilizada por Amnistía Internacional), y afirmó que ambos grupos, Citizen Lab y Amnesty Tech, habían «desarrollado una metodología sustancialmente similar para detectar la infraestructura del grupo NSO».[9] Cuatro de los autores del informe «CatalanGate» habían trabajado en la «Independent Peer Review of Amnisty's

*5/ Scott-Railton et al. CatalanGate página 22*

*6/* *El Periódico de España. El juez pide los móviles a los cargos de la CUP espiados para analizarlos. 27 de septiembre de 2022, https://www.epe.es/es/politica/20220927/juez-moviles-cargos-cup-espionaje-pegasus-75968035*

*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/*

*7/ Mr Deibert consideró esta validación como parte de la «revisión inter pares del informe» en su carta de 13 de mayo de 2022. Página 4.*

*8/* *Conjunto de herramientas de verificación móvil https://github.com/mvt-project/mvt*

*9/* *Bill Marczak, John Scott-Railton, Siena Anstis, and Ron Deibert (2017). Independent Peer Review of Amnesty International's Forensic Methods for Identifying Pegasus Spyware. Citizen Lab. 18 de julio de 2021 https://citizenlab.ca/2021/07/amnesty-peer-review/*

Forensic Methods for Identifying Pegasus Spyware». Recurrir a antiguos miembros de un equipo para el trabajo de «revisión *inter pares*» no cumple las normas académicas de validación externa. Menos aún cuando ambos equipos participan en validar mutuamente el trabajo de la otra parte.

El Sr. Maynier, alias Tek, trabajó en Citizen Lab entre 2016 y abril de 2021 y participó en varios informes de Citizen Lab relativos a Pegasus. Tenía una doble afiliación a Amnistía Internacional y Citizen Lab[10]. La investigación sobre Cataluña comenzó a más tardar en julio de 2020; por lo tanto, el Sr. Maynier trabajaba para Citizen Lab durante la investigación de CatalanGate, lo que le convierte en un experto inadecuado para llevar a cabo cualquier tipo de investigación externa e independiente. El Sr. Guarnieri, alias Nek, Senior Technologist de Amnistía Internacional, también estuvo doblemente afiliado y ejerció como investigador principal en Citizen Lab hasta al menos 2016[11].

La relación entre Citizen Lab y Amnistía Internacional es más profunda, como reconoce el Sr. Deibert en una declaración formal que ha participado en los grupos técnicos de Amnistía Internacional, y que Citizen Lab colabora de forma rutinaria con Amnistía Internacional[12].

*10/* *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/*

*Hi, I am Tek. About me.*
*https://randhome.io/about/*

*11/* *Claudio Guarnieri. re:publica.*
*https://re-publica.com/en/user/11930*

*Citizen Lab Senior Research Fellows at the 2016 Chaos Communications Congress, 26 de diciembre de 2016.*
*https://citizenlab.ca/2016/12/bill-marczak-john-scott-railton-speak-million-dollar-dissident-rest-us/*

*12/* *Statement of Ronald J. Deibert. Immigration Division. Immigration and Refugee Board of Canada, ID File No: 0018-C1-00135-01. UCI: 11-0952-9374. Statement in the context of Chelsea Manning's inadmissibility proceeding. Revisado el 16 de octubre de 2021*
*https://policycommons.net/artifacts/1961557/statement-of-ronald-j-deibert/2713322/https://re-publica.com/en/user/11930*

El Sr. Deibert afirma que Citizen Lab puede distinguir de manera fiable los intentos de infección por Pegasus de otros ataques con programas espía y hace referencia a seis años de investigación publicada, así como a validaciones independientes.[13] No obstante, en la lista de publicaciones de Citizen Lab no encontramos un único artículo revisado por pares. La «validación externa» de los análisis forénses figura en la mayoría de los informes realizados por Amnesty Tech; por ejemplo, en «Peace through Pegasus»[14], «Project Torogoz»,[15] «Pegasus vs. Predator»,[16] «Breaking the News»,[17] y «De Pearl a Pegasus».[18] Muchos de los demás informes de Citizen Lab, «FORCEDENTRY»,[19] «Análisis de la privacidad y la seguridad de la aplicación IATA de la tarjeta de viaje de Android»,[20] «Engrave Condition»,[21] «Pandemic Privacy»[22], «No Access»[23] y «Hooking Candiru»[24], ni siquiera se refieren a ningún proceso de validación externa.

13/ *Carta del Sr. Ronald Deibert al Sr. Jordi Cañas, página 4. https://deibert.citizenlab.ca/wp-content/uploads/2022/05/2022.05.13-L-Ferris-to-J-Canas.pdf*

14/ *Mohammed Al-Maskati, Bill Marczak, Siena Anstis, and Ron Deibert (2022) Peace through Pegasus Jordanian Human Rights Defenders and Journalists Hacked with Pegasus Spyware, Citizen Lab, 5 de abril de 2022 https://citizenlab.ca/2022/04/peace-through-pegasus-jordanian-human-rights-defenders-and-journalists-hacked-with-pegasus-spyware/*

15/ *John Scott-Railton, Bill Marczak, Paolo Nigro Herrero, Bahr Abdul Razzak, Noura Al-Jizawi, Salvatore Solimano, and Ron Deibert (2022). Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware, Citizen Lab, 12 de enero de 2022 https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/*

16/ *Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ron Deibert (2021). Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware, Citizen Lab, 16 de diciembre de 2021 https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/*

17/ *Bill Marczak, John Scott-Railton, Siena Anstis, Bahr Abdul Razzak, and Ron Deibert (2021). Breaking the News: New York Times Journalist Ben Hubbard Hacked with Pegasus after Reporting on Previous Hacking Attempts, Citizen Lab, 24 de octubre de 2021, https://citizenlab.ca/2021/10/breaking-news-new-york-times-journalist-ben-hubbard-pegasus/*

18/ *Bill Marczak, Ali Abdulemam1, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, John Scott-Railton, and Ron Deibert (2021). From Pearl to Pegasus Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits, Citizen Lab, 24 de agosto de 2021.*

19/ *Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ron Deibert (2021), FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild. Citizen Lab, 13 de septiembre de 2021, https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/*

20/ *Palleon Lin (2022). Privacy and Security Analysis of the IATA Travel Pass Android App. Citizen Lab, 13 de abril de 2022 https://citizenlab.ca/2022/04/privacy-and-security-analysis-of-the-iata-travel-pass-android-app/*

21/ *Jeffrey Knockel and Lotus Ruan (2022). Engrave Condition Apple's Political Censorship Leaves Taiwan, Remains in Hong Kong. Citizen Lab, 22 de marzo de 2022 https://citizenlab.ca/2022/03/engrave-condition-apples-political-censorship-leaves-taiwan-remains-in-hong-kong/*

22/ *Benjamin Ballard, Amanda Cutinha, and Christopher Parsons (2021). Pandemic Privacy A Preliminary Analysis of Collection Technologies, Data Collection Laws, and Legislative Reform during COVID-19. Citizen Lab, 28 de septiembre de 2021, https://citizenlab.ca/2021/09/pandemic-privacy-collection-technologies-data-collection-laws-and-legislative-reform-during-covid-19/*

23/ *Jakub Dalek, Nica Dumlao, Miles Kenyon, Irene Poetranto, Adam Senft, Caroline Wesley, Arturo Filastò, Maria Xynou, and Amie Bishop (2021). No Access LGBTIQ Website Censorship in Six Countries. Citizen Lab, 31 de agosto de 2021. https://citizenlab.ca/2021/08/no-access-lgbtiq-website-censorship-in-six-countries/*

24/ *Bill Marczak, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ron Deibert (2021). Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus. Citizen Lab, 15 de julio de 2021 https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/*

La larga colaboración entre Citizen Lab y Amnistía Internacional —y la de los miembros de sus equipos— debería reconocerse en los informes que han sido «revisados por pares» para que el lector sea consciente de las posibles limitaciones de este proceso de validación. Como ejemplo de buena práctica académica, no se les pide a los coautores revisar el trabajo del otro. Es más, a la hora de presentar publicaciones en revistas «revisadas por pares», a menudo se pide a los investigadores que declaren que no han trabajado previamente con los que sugieren como posibles revisores *inter pares*. La postura del Citizen Lab con respecto a la «revisión por pares» del informe CatalanGate parece carecer de rigor, ya que no se hizo explícito este reconocimiento de la estrecha colaboración (por otra parte, tampoco se hizo en la mayoría de sus resultados de investigación examinados).

No todos los informes se revisan por pares en el mundo académico. Con frecuencia, los autores proporcionan información y datos suficientes para que sus conclusiones puedan reproducirse o evaluarse. Sin embargo, alegar que un informe ha sido validado de forma independiente, cuando no es el caso, habida

cuenta de las relaciones entre las organizaciones, sus intereses compartidos, es inadecuado y contradice las buenas prácticas comúnmente consideradas en el mundo académico. El sitio web de la Universidad de Toronto sobre Integridad en la Investigación afirma que la política de la Universidad en lo que respecta a conducta ética exige que los miembros sigan «las normas más estrictas de conducta ética en todos los aspectos de la investigación, incluidas las solicitudes, las propuestas, la propia investigación, los informes y la publicación»[25].

Al preguntarse sobre la falta de replicabilidad y la ausencia de un repositorio o muestras que pudieran ser utilizadas por expertos independientes para validar los resultados, el Sr. Deibert hace alusión a la «credibilidad del testimonio» del Sr. Bill Marczak, investigador principal en Citizen Lab y desarrollador de la metodología técnica utilizada por Citizen Lab para identificar infecciones por Pegasus. Asimismo, afirma que:

> «Hasta la fecha, ningún análisis técnico de prestigio ha contradicho nuestras constataciones, ni se ha justificado ninguna preocupación específica en relación con nuestra metodología técnica para identificar a Pegasus».[26]

Sin embargo, no parece adecuado afirmar que «ningún análisis técnico de prestigio» ha contradicho sus resultados, dado que los análisis de Citizen Lab no son revisados por expertos independientes. Por otra parte, la credibilidad del trabajo académico científico no puede basarse en la reputación personal o profesional de los autores (o críticos), sino en el seguimiento de procesos transparentes y reproducibles, que suelen incluir la revisión *inter pares* o, al menos, la posibilidad de verificación externa.

Si el informe CatalanGate no puede ser falsificado[27] o validado, ¿cómo garantiza Citizen Lab que no contiene errores rele-

25/ *Universidad de Toronto (2019) Research Integrity https://research.utoronto.ca/research-integrity/research-integrity*

26/ *Carta del Sr. Ronald Deibert al Sr. Jordi Cañas, páginas 2-3.*

27/ *LeBel, E. P., Berger, D., Campbell, L., & Loving, T. J. (2017). Falsifiability is not optional. Journal of Personality and Social Psychology, 113(2), 254–261*

vantes? ¿Por qué Citizen Lab no facilitó ningún conjunto de datos que permitiera la validación independiente de sus hallazgos? ¿Por qué las muestras no estaban disponibles para los revisores *inter pares* fiables e independientes? Teniendo en cuenta que Citizen Lab compartió una muestra de 4 casos con Amnesty Tech, ¿podrían tener acceso otros revisores *inter pares* independientes a esas 4 muestras?

El Sr. Deibert afirma que la validación externa fue llevada a cabo por Amnesty Tech en marzo-abril de 2022.[28] El informe se publicó el 18 de abril de 2022, en una campaña de comunicación perfectamente coordinada, con infografías profesionales y costosas en 3 lenguas (inglés, catalán y español),[29] una exclusiva planificada con antelación por el Sr. Ronan Farrow en The New Yorker[30], vídeos,[31] un sitio web específico[32] y una cuenta de Twitter con 180 seguidores: @catalangate.[33] Dado que los primeros casos se identificaron y se anunciaron públicamente en julio de 2020, ¿por qué Citizen Lab esperó hasta marzo-abril de 2022 para llevar acabo la validación externa de los casos?

*28/ Carta del Sr Ronald Deibert al Sr. Jordi Cañas, página 4.*

*29/* *Would you click?*
*https://catalonia.citizenlab.ca/*

*30/* *Ronan Farrow (2022). How Democracies Spy on their Citizens. The New Yorker, 25 de abril de 2022*
*https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens*

*31/* *Assemblea. Catalan Gate, 26 de abril de 2022*
*https://www.youtube.com/watch?v=GGUr7Guk300*

*Assemblea Elisenda Paluzie #CatalanGate, 29 de abril de 2022, https://www.youtube.com/watch?v=G5TDEFBMYU0*

*32/* *CatalanGate Ens Estan Vigilant*
*https://catalangate.cat/*

*33/* *Catalangate, @catalangate,*
*https://twitter.com/catalangate*

Por lo general, la detección temprana de errores se utiliza para calibrar los instrumentos. ¿Habría revisado Citizen Lab su informe y suspendido la campaña de comunicación si alguna de las muestras analizadas por Amnesty Tech hubiera dado negativo o mostrado algún problema?

El informe CatalanGate reconoce que «nuestros métodos tienen una visión limitada de las infecciones de Android». Sin embargo, entre las presuntas víctimas iniciales, algunos, como el Sr. Roger Torrent eran propietarios de un dispositivo Android. Teniendo en cuenta esta debilidad instrumental reconocida, resulta sorprendente que no sometieran ninguno de los teléfonos Android supuestamente infectados a una validación externa.

Como intento de disipar las críticas formuladas por muchos académicos sobre el informe CatalanGate, algunas personas que defienden a Citizen Lab han alegado que su trabajo no puede juzgarse a la luz de las normas académicas, ya que su informe no es un trabajo académico, sino un informe de la industria[34].

**Infosec Nietzsche**
@nihlsec

En respuesta a **@joseolivas @citizenlab** y **2 más**

It's a threat intelligence report, not an academic paper. Maybe you need to spend some time learning the difference. Are you going to start attacking Mandiant and Verizon next for their non-academic threat intelligence reports?

4.12 PM · 18 de julio, 2022

**Marcus Hutchins**
@MalwareTechBlog

En respuesta a **@0x5adb07 @joseolivas** y **3 más**

Not only this, but did anyone see Citizen Lab claim their report was an academic study? Seems weird to project these requirements onto something that doesn't appear to have been published as such.

18:02 · 17 de julio, 2022

34/ **Philderbeast**
@thephilderbeast

En respuesta a **@joseolivas @jonathandata1** y **5 más**

The Cyberlab report is NOT academic work, it is industry report.

They have different standards and very different audiences, the fact that you can't see that shows how ignorant you are of the topic you're talking about

13 de julio, 2022

Sin embargo, estos argumentos están se contradicen con las escasas declaraciones públicas del Sr. Deibert en las que afirmaba la naturaleza académica de Citizen Lab, así como las frecuentes referencias a la necesidad de procedimientos de revisión *inter pares* que ha realizado en repetidas ocasiones.

**profdeibert**
@RonDeibert

We have always welcomed debate and dialogue about our work, but we condemn these sinister, underhanded activities in the strongest possible terms. Such a deceitful attack on an academic group like Citizen Lab is an attack on academic freedom everywhere.

25 de enero, 2019

**profdeibert**
@RonDeibert

Hi David. **@BBC** had referred to **@citizenlab** as a "firm" We are **@UofT @munkschool**. ie., academic group. **twitter.com/DaveLeeBBC/sta...**

> **Dave Lee** @DaveLeeDT · 26 de ago 2016
>
> Insomniacs! I'm on **@bbc5live** in a moment talking about this: **bbc.com/news/technolog...**

18:02 · 17 de julio, 2022

**profdeibert**
@RonDeibert

Funny -- talks about Governments versus Private Sector attribution of cyber espionage, but nothing about academic groups. Guess **@citizenlab** doesn't count? Also again I ask: why aren't there more **@citizenlab** like units in other Universities? **lawfareblog.com/private-sector...**

3:59 · 22 de diciembre, 2017

**profdeibert**
@RonDeibert

I trust **@UofT** admin, **@UTLaw** follow what's the most appropiate path forward now: restore the appointment offer. It is essential that the university is free from both external influences and appearances of external influence. The principle of academic freedom demands it.

19:20 · 8 de mayo, 2021

**profdeibert**
@RonDeibert

It is precisely to counter spurious claims like those of #hackingteam that careful, peer-reviewed academic research is vital. **@headhntr**

22:42 · 3 de noviembre, 2014

**profdeibert**
@RonDeibert

Universities have ethics review boards, w academic peer review. No place in University for "Security Officer". **twitter.com/mattblaze/stat...**

> **matt blaze** @mattblaze · 07 de oct 15
>
> **@bartongellman** I amb gladder every day that my university has no "site security offer" for me to answer to.

0:01 · 8 de octubre, 2015

Citizen Lab ha utilizado la «libertad académica» y la «independencia académica» como argumentos para disipar las críticas sobre sus métodos y la integridad de la investigación. Por ejemplo, en 2018, tras haber sido acusado de apropiación indebida de tecnología por parte de Sandvine, el abogado de Citizen Lab utilizó estos argumentos en una declaración enviada a la directora ejecutiva de las empresas en 2018, en la que se afirmaba que «incluso la percepción de que la agenda de investigación de la Universidad podría verse influida o socavada por los apoyos o las amenazas de una empresa privada es una amenaza para su independencia académica, credibilidad e integridad»[35].

De todos modos, esto parece contradecir el testimonio del Sr. Torrent, ni más ni menos que un líder político de Esquerra Republicana de Catalunya (ECR) y figura clave en el asunto CatalanGate, que afirmó en su libro que Citizen Lab estaba intentando reunir casos positivos de infecciones por Pegasus en Cataluña en nombre de Apple y como medio para alimentar los argumentos judiciales.[36]

Al parecer, Citizen Lab está reivindicando lo mejor de ambos mundos, es decir, ser capaz de operar bajo el paraguas de la Universidad de Toronto para reivindicar la libertad académica, al tiempo que rechaza la responsabilidad y la transparencia habituales en el mundo académico. De hecho, su investigación parece estar influida en cierta medida por agentes de la industria y activistas políticos partidistas, como demuestra este estudio.

35/ *Citizen Lab. Carta a Lyndon Cantor, consejero delegado de Paliare Roland Barristers, 8 de marzo de 2018.* *https://citizenlab.ca/wp-content/uploads/2018/03/UofT-Sandvine-Letter-to-Lyndon-Cantor-signed-8-March-2018.pdf*

36/ *Roger torrent (2021). Pegasus: L'Estat que ens espia. Barcelona: ARA Llibres, página 135.*

# 3

# Falta de transparencia

A pesar del presunto compromiso de Citizen Lab y de la Universidad de Toronto para mantener y solicitar los estándares más altos en términos de transparencia y rendición de cuentas públicas, el informe «CatalanGate» parece ser una excepción a la aplicación de estos principios. Como demuestra esta revisión crítica, existe una anormal falta de transparencia en relación con la metodología y los análisis utilizados por Citizen Lab en este caso.

Por ejemplo, la forma en que se repiten los ataques de Pegasus es muy inusual. En el «Apéndice A» del informe, en la sección de objetivos, aparecen 30 presuntas víctimas con fechas aproximadas de infecciones «en o alrededor del AAAA-MM-DD»; en el caso de 5 presuntas víctimas hay un intervalo de tiempo («algún tiempo entre AAAA-MM-DD y AAAA-MM-DD»); en 12 casos no hay más información más allá de «[incapaz de determinar la(s) fecha(s) de infección específica]»; en 1, hay [«Fecha (s) de infección desconocida]; en 8 casos simplemente se notifica que la víctima había recibido «Pegasus SMSes»; y en 5 casos solo hay una nota en la que se afirma que estas presuntas víctimas habían recibido «2019 notificaciones de Pegasus de WhatsApp». La información facilitada por Citizen Lab no permite a los lectores saber cuántas de estas presuntas víctimas han sido analizadas por medios forenses ni cuáles fueron los resultados. Del mismo modo, en lo que respecta a la presunta infección de Candiru, hay 3 presuntas víctimas que aparecen como objetivo y una como infectada. Por otra parte, el informe no explica claramente las implicaciones de esas etiquetas. ¿Por qué Citizen Lab no indica claramente cuántas de las presuntas víctimas han dado negativo a la infección, es decir, no han sido infectadas, y si examinaron de forma forénsica los dispositivos de todos los políticos y activistas de la lista? La forma en que Citizen Lab agrupa los casos con resultados negativos de infección con otros con resultados positivos de infección, e incluso añade casos en los que no está claro si se llevó a cabo algún análisis, muestra una clara falta de rigor.

Las imprecisiones y omisiones de Citizen Lab en relación con las principales opciones y procesos metodológicos están en contradicción con algunas de las directrices generales y los cinco principios del análisis forense digital prescritos por la Agencia europea para la Ciberseguridad (ENISA).

ENISA, como la mayoría de los organismos especializados en investigación digital, sostiene que «la incautación, la custodia, el control, el traslado, el análisis y la disposición de las pruebas deben documentarse cronológicamente de una manera adecuada que constituya una «cadena de custodia»[37]. Solicita que las pruebas sean tramitadas por especialistas: «Cada dispositivo tiene sus características y sus procedimientos de manipulación deben ajustarse a ellos: Los dispositivos electrónicos son especialmente sensibles a los cambios no intencionados en su estado, lo que, junto con otros peligros, puede dar lugar a la reversión de las pruebas por parte del Tribunal de Justicia».[38] Como demostrará esta revisión en secciones posteriores, las pruebas fueron gestionadas no solo por especialistas en informática forense, sino también por algunos activistas proseparatismo como el Sr. Elies Campo, que no contaba con una formación previa conocida en criminalística digital. En el proceso podrían haberse producido alteraciones involuntarias o intencionadas de las pruebas.

ENISA también insiste en el uso de procedimientos, técnicas y herramientas adecuados: «junto con los conocimientos especializados de los ingenieros forenses, cada tarea requiere seguir los procedimientos y aplicar técnicas adecuadas con herramientas adecuadas. Cada investigación forense debe ser rastreable y repetible por otros especialistas forenses con la misma conclusión final».[39]

El informe CatalanGate, al igual que muchos otros informes del Citizen Lab, no documenta de forma mínima las técnicas y procedimientos forenses, y sería imposible para cualquier otro especialista forense rastrear y reproducir el análisis. Por el contrario, cuando se le preguntó directamente sobre fechas, procedimientos de muestreo y protocolos para el manejo de pruebas, Citizen Lab dio respuestas anormalmente vagas y elusivas.[40] El trabajo de campo fue realizado en Cataluña por el Sr. Campo y otros activistas y políticos proseparatismo. Aunque el Sr. Campo fue supervisado desde Toronto por los Sres. Deibert y Scott-Railton, no hay rastro de ningún protocolo escrito ni técnica forense aplicada para el trabajo de campo.

«Exhaustividad» es otro criterio promovido por ENISA, es decir, las pruebas «deben abarcar el caso con total independencia de la perspectiva».[41] En este caso, es evidente que solo se sometieron a análisis los teléfonos de políticos y activistas separatistas.

*37/* *Universidad de Toronto (2019) Research Integrity* *https://research.utoronto.ca/research-integrity/research-integrity*

*38/* *Carta del Sr. Ronald Deibert al Sr. Jordi Cañas, páginas 2-3.*

*39/* *ENISA (2013) Digital forensics, página 3.*

*40/* *Vea, por ejemplo, la carta del Sr. Ronald Deibert al Sr. Jordi Cañas. 13 de mayo de 2022.*

*41/* *ENISA (2013) Digital forensics, página 3.*

Esto se debe en gran medida a la participación de organizaciones y partidos políticos separatistas en la selección de datos. No consta si se han analizado otros teléfonos o grupos de control. Citizen Lab se niega a comunicar los resultados negativos y el número de análisis realizados.

ENISA también hace hincapié en que existen cinco principios que sientan las bases para todas las operaciones de evidencia electrónica, como en este caso: 1) integridad de los datos, 2) pista de auditoría, 3) apoyo especializado, 4) formación adecuada, y 5) legalidad. La integridad de los datos recuerda a los investigadores que deben conservar una cadena de custodia forense. En el informe CatalanGate no se hace referencia alguna a la cadena de custodia. En relación con el principio de la pista de auditoría, ENISA afirma que «es imperativo registrar con precisión todas las actividades para que un tercero pueda reconstruir las acciones del primer interviniente en la escena con el fin de garantizar su valor probatorio ante los tribunales. Toda actividad relacionada con la incautación, el acceso, el almacenamiento o la transferencia de pruebas electrónicas deberá estar plenamente documentada, conservada y disponible para su revisión.»[42] Como se ha mencionado anteriormente, no se dispone de documentación para la revisión o registro del acceso, almacenamiento o transferencia de pruebas electrónicas. No se explica cuándo ni cómo se recogieron las pruebas ni por quién. ENISA pide que todas las personas implicadas en el proceso tengan los conocimientos especializados y experiencia necesarios en la materia, los conocimientos de investigación necesarios y los conocimientos jurídicos necesarios.[43] No se hace referencia a la formación o a las capacidades y experiencia especializadas del Sr. Campo, que coordinó el trabajo de campo y recopiló pruebas en nombre de Citizen Lab. Por el contrario, al preguntarse qué tipo de conocimientos técnicos o competencias sirvieron de base para elegir al Sr. Elies Campo como coordinador del trabajo de campo en Cataluña, el Sr. Deibert respondió que, para él, no se requieren conocimientos técnicos especiales.[44] Como otros participantes y el Sr. Campo han reconocido públicamente[45], el Sr. Campo participó directamente en la detección de infecciones y la recogida de pruebas, y, por tanto, según ENISA, debería haber recibido formación o haber tenido experiencia previa.

*42/ ENISA (2013) Digital forensics, página 5.*

*43/ ENISA (2013) Digital forensics, página 5.*

*44/ Carta del Sr. Ronald Deibert al Sr. Jordi Cañas, página 5.*

*45/* *Véase, por ejemplo, CCMA.Cat. TV3. Preguntes Freqüents. El Catalangate amb John Scott-Railton i Elies Campo, Lang Lang i Noemí Casquet, 23 de abril de 2022; https://www.ccma.cat/tv3/alacarta/preguntes-frequents/el-catalangate-amb-john-scott-railton-i-elies-campo-lang-lang-i-noemi-casquet/video/6155478/.*

Además de los principios y directrices de ENISA, el trabajo de Citizen Lab, al menos en el caso de la investigación «CatalanGate», contraviene aspectos pertinentes del Protocolo de Berkeley sobre investigaciones digitales abiertas preconizadas por la Oficina de las Naciones Unidas del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Por ejemplo, este protocolo establece lo siguiente:

«Una gestión y un tratamiento adecuados de este material aumentarán considerablemente la probabilidad de que pueda ser utilizado por fiscales y asesores. Sin embargo, si se utilizan métodos poco sólidos de recogida y conservación, la información no puede considerarse fiable a efectos de la determinación de los hechos en un caso concreto. Los órganos jurisdiccionales y los mecanismos de investigación se beneficiarán de criterios claros para evaluar el peso de la información de código abierto, ya sea como enlace o como prueba basada en delitos».[46]

*46/* *United Nations (2022). 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. Página V.* *https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf*

Al igual que los principios de la ENISA, el Protocolo de-Berkeley establece la pertinencia de los métodos de recopilación de datos y de conservación de los datos, que en el caso del informe «CatalanGate» no se han revelado ni siquiera tras un interrogatorio. Por otra parte, considera que:

«[e]n cumplimiento de los principios profesionales relacionados con las investigaciones digitales de código abierto, los investigadores deben garantizar que son responsables, competentes y objetivos».[47]

Ninguno de estos tres principios parece cumplirse en el caso de la investigación «CatalanGate». El protocolo de Berkeley indica que:

«la transparencia en los métodos y procedimientos de investigación es un elemento esencial para garantizar la rendición de cuentas. Así pues, en la medida de lo posible y razonable, los investigadores de código abierto deben mantener registros de sus actividades».[48]

La ausencia de registros sobre la recogida y el tratamiento de datos, así como la falta de competencias especializadas y de formación específica reconocida por Citizen Lab en el caso del Sr. Campo son indicadores claros de la violación de los dos primeros principios profesionales.

*47/ United Nations Berkeley Protocol, página 9.*
*48/ United Nations Berkeley Protocol, página 11.*

Sin embargo, la infracción más flagrante aparece en el caso del principio de objetividad.

«Los investigadores de código abierto deben comprender el potencial de sesgos personales, culturales y estructurales que pueden afectar a su trabajo y la necesidad de adoptar contramedidas para garantizar la objetividad».[49]

En el presente caso, es evidente que confiar la coordinación del trabajo de campo a un activista político que afirma ser víctima de programas espía constituye una contradicción con el principio de objetividad. Este asunto es aún más grave si se tiene en cuenta que el Sr. Campo fue el segundo autor del informe y que no se reflejó en él ninguna cláusula de exención de responsabilidad ni reconocimiento de sus actividades como activista a favor de la secesión. Además, no se adoptaron contramedidas para mitigar su evidente sesgo. Su participación en el informe parece formar parte de su trabajo como activista político, ya que fue él quien contactó con Citizen Lab ofreciendo ayuda para encontrar casos de ataques de Pegasus entre otros activistas y políticos secesionistas.[50]

Otro aspecto relacionado que el Protocolo de Berkeley defiende es el siguiente:

«Los investigadores deben asegurarse de que enfocan sus investigaciones de manera objetiva, desarrollan y despliegan múltiples hipótesis de trabajo y no favorecen ninguna teoría concreta que explique sus casos».[51]

*49/ United Nations Berkeley Protocol, página 11.*
*50/ Véa, por ejemplo, Preguntes Freqüents, 23 de abril de 2022, o la carta del Sr. Ronald Deibert al Sr. Jordi Cañas, página 5.*
*51/ United Nations Berkeley Protocol,*

Citizen Lab solo tiene en cuenta la hipótesis del espionaje ilegal por parte del Gobierno español y las fuerzas de seguridad. Como se explica más adelante, ni siquiera se mencionan otras hipótesis verosímiles. Entre ellas se incluye el seguimiento previa autorización judicial lo que, sin duda, ocurrió en un número considerable de presuntas víctimas[52]; la posibilidad de que algunas presuntas infecciones fueran causadas por *malware* o *spyware*;[53] o que los servicios secretos de Rusia u otros países afectados por la colaboración de algunas de las presuntas víctimas con los emisarios del Kremlin podrían haberles espiado.[54] Citizen Lab, en su informe CatalanGate, no intentó descartar hipótesis alternativas y simplemente confirmó la inicial, basada en lo que admiten como «evidencia circunstancial». Esta hipótesis era conveniente para Citizen Lab, ya que se especializan en Pegasus, tras haber publicado docenas de informes sobre este programa espía específico comparativamente, han estudiado mucho menos casos causados por otros programas maliciosos[55].

52/ *20 minutos. El CNI confirma que investigó a una veintena de independentistas, entre ellos. 6 de mayo de 2022, https://www.20minutos.es/noticia/4995670/0/la-directora-del-cni-admite-el-espionaje-legal-a-18-independentistas-incluido-pere-aragones/*

53/ *Techtarget.Top 10 spyware threats, mayo de 2022, https://www.techtarget.com/whatis/definition/Top-10-Spyware-Threats*

54/ *El Periódico. El enlace de Puigdemont ofreció a Rusia reconocer Crimea a cambio de apoyo a la independencia de Catalunya. 21 de noviembre de 2019, https://www.elperiodico.com/es/politica/20191121/terradellas-puigdemont-rusia-crimea-dui-catalunya-7741883*

55/ *Citizen Lab. Publications. https://citizenlab.ca/publications/*

*Citizen Lab. Targeted Threats. https://citizenlab.ca/category/research/targeted-threats/page/6/*

Esta también fue útil para activistas y organizaciones secesionistas en sus intentos de mostrar a España como responsable de mala conducta, represión y de tener estándares democráticos cuestionables, estrategia que han seguido desde hace muchos años.[56]

Por último, el National Institute of Standards and Technology (NIST) de las directrices de dispositivos móviles del Departamento de Comercio de Estados Unidos está de acuerdo con los principios básicos defendidos por ENISA y la OHCHR, y subraya la importancia de los procedimientos y los requisitos de documentación que faltan en esta investigación de Citizen Lab. Las directrices de esta organización hacen referencia a la necesidad de documentar con precisión y aislar todos los datos visibles sobre cómo se encuentran los dispositivos móviles. En particular, estas organizaciones recomiendan desactivar la red, incluyendo:

«Los datos entrantes (llamadas o mensajes de texto) que puedan modificar el estado actual de los datos almacenados en el dispositivo móvil [...]. Los examinadores forenses deben ser conscientes y tomar precauciones a la hora de proteger los dispositivos móviles paramitigar las posibilidades de modificación de los datos».[57]

56/ *Hernández, G., & Closa, C. (2022). The challenge of Catalan secessionism to the European model of the rule of law. Hague Journal on the Rule of Law, 1-29; Cardenal, J.P. (2020). La telaraña. La trama exterior del procés. Barcelona: Editorial Ariel; European Parliament Debates. Whitewashing of the anti-European extreme right in the EU (topic debate). Clara Ponsatí Obiols, 19 de octubre de 2022,* https://www.europarl.europa.eu/doceo/document/CRE-9-2022-10-19-INT-3-149-0000_EN.html

*Carles Puigdemont, The Catalan Independence Movement Has Proven Its Strength. Now Spain's Government Must Talk to Us. Time. 21 de octubre de 2019.* https://time.com/5705915/carles-puigdemont-catalan-protest-barcelona/

57/ *Ayers,R., Brothers, S. & Jansen, W. (2014). Guidelines on Mobile Device Forensics. NIST Special Publication 800-101. Revision 1. Página 28.* http://dx.doi.org/10.6028/NIST.SP.800-101r1,

No hay pruebas de que Citizen Lab llevara un registro preciso de cómo se encontraron físicamente los dispositivos, y parece probable que ningún empleado de Citizen Lab más allá del Sr. Campo tuviera acceso directo a ninguno de los teléfonos y ordenadores analizados. Y lo que es más importante, no hay pruebas de que los dispositivos estuvieran aislados o desconectados de las redes entre los análisis preliminares y los análisis forenses remotos que, presumiblemente, realizaban los empleados de Citizen Lab. Si estos teléfonos estuvieran efectivamente infectados con programas espía o programas maliciosos, las pruebas podrían haberse alterado en el proceso. Al menos uno de los participantes en el estudio admite que meses después de que su teléfono diera negativo, fue contactado de nuevo por el Sr. Campo, que finalmente encontró pruebas de los ataques de Pegasus, que databan de antes del primer análisis[58].

El NIST recomienda un análisis físico del producto, incluido el embalaje, el transporte y el almacenamiento de pruebas, mencionando que el especialista forense debe precintar el producto en un contenedor adecuado; también debe haber una custodia de las pruebas. El NIST se refiere a los beneficios del «proceso de triaje *in situ*»: se trata de la extracción *in situ* (manual o lógica), pero sus orientaciones expresan prejuicios por el entorno y la transformación de los laboratorios.[59] La decisión de Citizen Lab de no analizar físicamente en su laboratorio a ninguna de las presuntas víctimas de CatalanGate no está justificada en su informe.

*58/* *Assemblea. Jordi Sànchez #CatalanGate. 26 de abril de 2022,* *https://youtu.be/9crBYexH6Ew*

*59/* *Ayers,R., Brothers, S. & Jansen, W. (2014). Guidelines on Mobile Device Forensics, páginas 33-40.*

El NIST hace alusión a la guía de examen forense de pruebas digitales del Departamento de Justicia de los Estados Unidos para recomendar el registro sistemático de las personas que crearon, modificaron o accedieron a un expediente, así como el calendario, y proporciona recomendaciones sobre la notificación de exámenes forenses, en particular:[60]

- → *Identidad de la agencia informadora*
- → *Identificador del caso o número de presentación*
- → *Investigador del caso*
- → *Fecha de recepción de las pruebas*
- → *Fecha del informe*
- → *Lista descriptiva de los elementos presentados para su examen, incluido el número de serie, la marca y el modelo*
- → *Identidad y firma del examinador*
- → *El equipo y la configuración utilizados en el examen*
- → *Breve descripción de las medidas adoptadas durante el examen, como búsquedas por cadena, búsquedas de imágenes gráficas y recuperación de archivos borrados*
- → *Materiales de apoyo, como copias impresas de elementos de prueba concretos, copias digitales de pruebas y documentación sobre la cadena de custodia*
- → *Detalles de las constataciones*
- → *Conclusiones del informe*

El informe CatalanGate omite la mayor parte de esta información y Citizen Lab tampoco la ha compartido después de ser preguntado al respecto.[61] No puede preverse ninguna explicación razonable para la objeción de compartir información sobre cuándo, dónde, cómo y por quién fueron los dispositivos analizados. Como se explica más adelante, las contradicciones encontradas en los testimonios sobre los agentes implicados en el examen técnico de los teléfonos y ordenadores parecen confirmar que en esta investigación no se observaron muchos principios comúnmente aceptados en la ciencia y la criminalística digital.

En particular, la falta de referencias a la cadena de custodia o a las precauciones adoptadas para garantizar que no se haya alterado la evidencia (física y lógica) indica un proceso poco riguroso que normalmente invalida los datos recogidos, lo que le impide informar cualquier decisión jurídica.

*60/* *Ayers,R., Brothers, S. & Jansen, W. (2014). Guidelines on Mobile Device Forensics, páginas 51 y 56. Mukasey, M.B., Sedgwick, J.L. & Hagy, D.W. (2008). Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, NCJ 219941, Abril de 2008, U.S. Department of Justice Office of Justice Programs*
https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

*61/ Carta de Ronald Deibert al Sr. Jordi Cañas ofrece un ejemplo de respuestas elusivas en relación con las preguntas.*

La falta de transparencia y rigor académico también queda ilustrada por las modificaciones introducidas por Citizen Lab en el informe tras su publicación. Algunos de estos cambios todavía no han sido notificados en ningún registro (cuadro 3). Por precaución, el autor de este informe había descargado la versión original. Posteriormente, Citizen Lab añadió un párrafo que modificaba una declaración engañosa del original que afirmaba que «las revelaciones de Snowden de 2013 revelaron que la NSA había interceptado 60 millones de llamadas en España entre diciembre de 2012 y enero de 2013». También modificaron la fecha de infección del Sr. Botran. En junio de 2022, la fecha de infección del dispositivo del Sr. Andreu Van den Eynde también se modificó en el cuerpo del informe. No obstante,Citizen Lab ha admitido un error y eliminado de la lista de presuntas víctimas D. Antoni Comín el 22 de diciembre de 2022.[62] El sitio web CatalanGate.cat aún no ha eliminado al Sr. Comín de la lista de presuntas víctimas.[63]

62/

*Ron Deibert (2022). CatalanGate Report Correcting a Case. 22 de diciembre de 2022*
*https://citizenlab.ca/2022/12/catalangate-report-correcting-a-case/*

63/

*CatalanGate.cat. Víctimas de CatalanGate. https://catalangate.cat/en/#victimes, consultado por última vez el 4 de diciembre de 2022.*

## TABLA 1

## TEXTO DEL INFORME CATALANGATE EL 18 DE ABRIL DE 2022 Y EL 29 DE NOVIEMBRE DE 2022[64]

| | | | | | |
|---|---|---|---|---|---|
| **Abusos de vigilancia documentados en España y Cataluña**<br><br>Aunque el secreto afecta a las prácticas de vigilancia de España, en las últimas décadas han salido a la luz una serie de casos que son pertinentes para este informe y demuestran un historial de vigilancia nacional y el uso de programas espía por parte de las autoridades españolas. En 2001, Mariano Rajoy, entonces ministro del interior de España, adquirió el Sistema integral de interpretación de las comunicaciones (SITEL), el programa espía utilizado por la Guardia Civil y el CNI para rastrear los teléfonos de los sospechosos. Al parecer, España también «coludió» con la Agencia Nacional de Seguridad (NSA) de los Estados Unidos. Las revelaciones de Snowden de 2013 revelaron que la NSA había interceptado 60 millones de llamadas en España entre diciembre de 2012 y enero de 2013.<br><br>Según el Confidencial, el CNI y la Policía Nacional pagaron al menos 209.000 EUR a la empresa informática de vigilancia Hacking Team basada en Milán por el uso de su programa espía en 2010. La compra se reveló por primera vez en 2015 cuando WikiLeaks publicó correos electrónicos internos de Hacking Team. El País informó entonces de que el contrato con el CNI era «válido de 2010 a 2016, por valor de 3,4 millones de euros». El CNI reconoció que compraba el programa espía en aquel momento, afirmando que lo hizo «de conformidad con las leyes de contratación del sector público». El CNI se negó a facilitar más información sobre lo que hizo con el programa espía de Hacking Team. En 2015, Citizen Lab cartografió la proliferación de Finfisher, un sofisticado software de programas espía de ordenador vendido exclusivamente a los gobiernos con fines de inteligencia y de aplicación de la ley, e identificó a un presunto cliente español. | | | **Abusos de vigilancia documentados en España y Cataluña**<br><br>Aunque el secreto afecta a las prácticas de vigilancia de España, en las últimas décadas han salido a la luz una serie de casos que son pertinentes para este informe y demuestran un historial de vigilancia nacional y el uso de programas espía por parte de las autoridades españolas. En 2001, Mariano Rajoy, entonces ministro del interior de España, adquirió el Sistema integral de interpretación de las comunicaciones (SITEL), el programa espía utilizado por la Guardia Civil y el CNI para rastrear los teléfonos de los sospechosos. Al parecer, España también «coludió» con la Agencia Nacional de Seguridad (NSA) de los Estados Unidos. Las revelaciones de Snowden de 2013 revelaron que la NSA había interceptado 60 millones de llamadas en España entre diciembre de 2012 y enero de 2013. Sin embargo, un análisis posterior mostrado entre esas afirmaciones, estaba basado en una posible interpretación errónea de las diapositivas de las revelaciones de Snowden y, en realidad, estaba relacionado con la recopilación de datos por parte de aliados de la OTAN, incluida España, en Afganistán.<br><br>Según el Confidencial, el CNI y la Policía Nacional pagaron al menos 209.000 EUR a la empresa informática de vigilancia Hacking Team basada en Milán por el uso de su programa espía en 2010. La compra se reveló por primera vez en 2015 cuando WikiLeaks publicó correos electrónicos internos de Hacking Team. El País informó entonces de que el contrato con el CNI era «válido de 2010 a 2016, por valor de 3,4 millones de euros». El CNI reconoció que compraba el programa espía en aquel momento, afirmando que lo hizo «de conformidad con las leyes de contratación del sector público». El CNI se negó a facilitar más información sobre lo que hizo con el programa espía de Hacking Team. En 2015, Citizen Lab cartografió la proliferación de Finfisher, un sofisticado software de programas espía de ordenador vendido exclusivamente a los gobiernos con fines de inteligencia y de aplicación de la ley, e identificó a un presunto cliente español. | |
| Albert Botrán | Miembro del Congreso de los Diputados de España, Candidatura de Unitat Popular | Ese día, o por esas fechas 01-12-2020 | Albert Botrán | Miembro del Congreso de los Diputados de España, Candidatura de Unitat Popular | Ese día, o por esas fechas 01-12-2020 |
| El teléfono de Andreu Van den Eynde, abogado de los destacados secesionistas catalanes Oriol Junqueras, Roger Torrent, Raül Romeva y Ernest Maragall, fue infectado el 14 de junio de 2020. El dispositivo de Jaume Alonso-Cuevillas, abogado que también representaba a Puigdemont, estaba infectado por Pegasus, aunque no pudimos determinar la fecha de la infección. En la actualidad, Alonso-Cuevillas es miembro del Parlamento de Cataluña, antiguo decano del Colegio de Abogados de Barcelona y antiguo presidente de la Federación Europea de Abogados.<br><br>**Objetivo: Generalitat de Catalunya, Parlamento y Políticos**<br><br>Los dispositivos de los políticos secesionistas catalanes fueron infectados ampliamente con Pegasus. Fueron objetivo de la infección a lo largo de negociaciones delicadas entre los Gobiernos catalán y español. En esta sección se enumera una selección de los casos. | | | El teléfono de Andreu Van den Eynde, abogado de los destacados catalanes Oriol Junqueras, Roger Torrent, Raül Romeva y Ernest Maragall, fue infectado el 14 de mayo de 2020. El dispositivo de Jaume Alonso-Cuevillas, abogado que también representaba a Puigdemont, estaba infectado por Pegasus, aunque no pudimos determinar la fecha de la infección. En la actualidad, Alonso-Cuevillas es miembro del Parlamento de Cataluña, antiguo decano del Colegio de Abogados de Barcelona y antiguo presidente de la Federación Europea de Abogados.<br><br>**Objetivo: Generalitat de Catalunya, Parlamento y Políticos**<br><br>Los dispositivos de los políticos catalanes fueron infectados ampliamente con Pegasus el 14 de mayo de 2020. Fueron objetivo de la infección a lo largo de negociaciones delicadas entre los Gobiernos catalán y español. En esta sección se enumera una selección de los casos. | | |

*64/ 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-operation-against-catalans-using-pegasus-candiru/*

Citizen Lab tampoco ha sido muy claro sobre cómo se financió la investigación en Cataluña. El Sr. Deibert explica que toda participación en el programa de investigación de las presuntas víctimas del programa espía Pegasus es voluntaria y no remunerada y afirma que las fuentes de financiación de Citizen Lab son públicas en su página web.[65] Sin embargo, su web solo indica los nombres de algunos contribuyentes y no detalla los importes que cada uno de ellos les concede. Además, su web ofrece enlaces al «Citizen Lab Fund»[66], en el que los donantes pueden hacer regalos a Citizen Lab. Estos pueden hacerse anónimanente. Además, como se explica más adelante, la Universidad de Toronto está mostrando una gran reticencia a revelar esta información. El autor de este informe presentó una solicitud de Ley de Libertad de Información y Protección de la Privacidad (FIPPA) en julio de 2022 y consiguió obtener información sobre los ingresos recibidos por el Citizen Lab.

Sin embargo, se han negado a identificar las organizaciones o individuos que les proporcionaron cada una de las líneas de financiación (véase el cuadro 4). Citizen Lab ha conseguido aumentar su financiación anual de manera muy significativa desde 2019, pasando de 1.750.135 CAD para el curso académico 2019-2020, cuando comenzaron las investigaciones de WhatsApp y Cataluña, a 3.713.603 CAD en 2021-22. Se trata de un aumento del 112 % que, dada la falta de información precisa de la Universidad de Toronto, este informe no puede atribuir a ninguna institución o persona concreta. Tampoco es posible calcular qué parte de los ingresos de Citizen Lab proviene de organizaciones privadas, públicas, sin ánimo de lucro o corporativas. Este es el caso de al menos una parte de la financiación obtenida por Citizen Lab a través de la Fundación Ford de Apple Inc.[67]

65/ *Citizen Lab. About.*
*https://citizenlab.ca/about/*

66/ *Munk School of Global Affairs & Public Policy*
*Citizen Lab Fund*
*https://engage.utoronto.ca/site/SpageServer?pagename=donate#/fund/847*

67/ *Apple. Newsroom, 22 de julio de 2022*
*https://www.apple.com/uk/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/*

## TABLA 2

### FINANCIACIÓN DE CITIZEN LAB[68]

| Fecha de finalización | Financiación total | | 2017-18 | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022-23 |
|---|---|---|---|---|---|---|---|---|
| | USD otros | CAD | | | | | | |
| 31.12.2021 | 1.000.000 | 1.304.917 | | 328.049 | 327.718 | 649.150 | | |
| 31.10.2021 | 1.400.000 | 1.800.630 | 450.170 | 450.170 | 450.170 | | | |
| 31.07.2021 | 450.000 | 586.845 | | 191.703 | 195.876 | 199.266 | | |
| 31.11.2021 | 300.000 | 503.790 | | 167.930 | 167.930 | 167.930 | | |
| 31.01.2022 | [redacted] | 355.950 | | | 124.300 | 141.250 | 72.902 | |
| 31.12.2022 | 360.000 | 468.540 | | | 156.180 | 156.180 | 156.180 | |
| 31.12.2022 | 350.977 | 487.469 | 104.167 | 227.875 | 41.667 | | | |
| 31.12.2020 | 150.000 | 200.910 | | 200.910 | | | | |
| 31.10.2021 | 1.100.000 | 1,443.310 | | 949.181 | | 494.129 | | |
| 31.05.2022 | 100.000 | 120.420 | | | | | 120.420 | |
| 30.11.2024 | 1.400.000 | 765.585 | | | | | 255.195 | |
| 31.12.2025 | 450.000 | 1.521.600 | | | | | 380.400 | |
| 28.12.2025 | | 952.650 | | | | | | 317.550 |
| 31.03.2025 | 750.000 | 375.240 | | | | | | |
| [redacted] | 300.000 | 954.295 | 40.362 | 41.167 | 41.972 | 42.828 | 47.196 | |
| [redacted] | 850.000 | 664.600 | 274.093 | | | | | |
| 30.09.2020 | 540.000 | 381.176 | | 189.515 | 191.661 | | | |
| 30.09.2022 | 290.000 | 367.744 | | | | 191.801 | 175.943 | |
| [redacted] | 25.000 | 33.343 | | | 33.343 | | | |
| [redacted] | 200.000 | 251.500 | | | | 251.500 | | |
| [redacted] | [redacted] | 25.000 | | 5.000 | 10.000 | 10.000 | | |
| [redacted] | 16.525 | 21.040 | | | | 21.040 | | |
| | | 10.000 | | | | | 10.000 | |
| | | 100.000 | | | | | 100.000 | |
| | | 89.779 | 2.984 | 3.565 | 9.319 | 21.980 | 44.575 | 7.357 |
| 31.12.9999 | | 1.150.000 | | | | | 1.150.000 | |
| 31.12.9999 | | 750.000 | | | | | 750.600 | |
| | **8.922.502** | **15.686.381** | **871.776** | **2.755.065** | **1.750.135** | **2.347.054** | **3.713.603** | **324.907** |

*68/ Anexo de carta en respuesta a la solicitud n.º #22-0052 de la FIPPA, recibida el 22 de agosto de 2022. La Universidad de Toronto se ha negado repetidamente a proporcionar los nombres de cualesquiera de las instituciones e individuos que le financian y que aparecen en esta tabla.*

# 4

# Una confianza anormal en la fiabilidad de la metodología y rechazo de posibles falsos positivos

En una entrevista a El País, el Sr. Deibert afirmó que contaba con un «100 % de fiabilidad de los ataques que hemos registrado». A continuación, los periodistas le preguntaron: «¿Podría haber falsos positivos?» a lo que respondió «No. Nuestros métodos son muy precisos y han sido desarrollados a lo largo de los años»[69].

Sin embargo, la literatura académica revisada por pares sobre la criminalística digital y la detección de programas maliciosos trata constantemente el problema de los «falsos positivos» (por ejemplo, Abela *et al.* 2013; Alherbawi *et al.* 2013; Pandey *et al.* 2018);[70] esto también implica importantes consideraciones de ética en la investigación. En el contexto de la creciente presión para publicar, hay pocos incentivos para probar la existencia de falsos positivos, ya que cuanto mayor sea el número de infecciones, mayor será el impacto del artículo y será más fácil atraer la atención de los medios de comunicación y más financiación para el centro de investigación.[71]

*69/*

*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-usan-pegasus-porque-tienen-apetito-de-espiar.html*

*ElDiario.es. El juez investiga si Vendrell y Madí contactaron con el Govern para «obtener contratos de emergencia» por la COVID-19. 29 de octubre de 2020,*
*https://www.eldiario.es/catalunya/juez-investiga-si-vendrell-madi-contactaron-govern-obtener-contratos-emergencia-covid-19_1_6370775.html*

*70/* *Abela, K. J., Angeles, D. K., Alas, J. R. D., Tolentino, R. J., & Gomez, M. A. (2013). An automated malware detection system for android using behavior-based analysis AMDA. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2(2), 1-11.; Alherbawi, N., Shukur, Z., & Sulaiman, R. (2013). Systematic literature review on data carving in digital forensic. Procedia technology, 11, 86-92; Pandey, P., Almodaresi, F., Bender, M. A., Ferdman, M., Johnson, R., & Patro, R. (2018). Mantis: a fast, small, and exact large-scale sequence-search index. Cell systems, 7(2), 201-207.*

*71/*

*Academia Enango. ¿Por qué los falsos resultados positivos son nocivos para la investigación científica? 3 de mayo de 2022*
*https://www.enago.com/academy/why-false-positive-results-are-harmful-to-scientific-research/*

Existen varios informes que muestran que los falsos positivos son una posibilidad probable en la detección forense para los dos productos mencionados en el informe CatalanGate, Candiru y Pegasus.[72]

Además, se sabe que la herramienta de detección de programas espía «MVT» de Amnesty Tech ha sido inducida fácilmente a error (falso positivo).[73] Incluso Amnesty Tech ha admitido en varias ocasiones el problema de los falsos positivos y ha modificado su herramienta de detección de programas espía en consecuencia: por ejemplo, al eliminar los indicadores de compromiso (OIC)[74] y los dominios.[75] Errores en los COI fueron detectados en las muestras que Citizen Lab les envió para su validación,[76] lo que también confirma que los métodos de Citizen Lab están lejos de ser infalibles.

Esta postura poco ortodoxa en materia de investigación científica también plantea varias cuestiones a la Universidad de Toronto y a la Escuela Munk de Asuntos Globales de Política Pública, que acogen y supuestamente supervisan el trabajo del Citizen Lab: ¿la Universidad de Toronto supervisa o produce a menudo investigaciones científicas con una fiabilidad del 100 % y en las que no hay riesgo de «falsos positivos»? ¿Respalda la Universidad de Toronto el carácter «infalible» del trabajo de Citizen Lab? ¿Dispone la Universidad de Toronto de algún sistema para garantizar que estas publicaciones no verificables externamente no contienen errores ni inducen a error?

*72/* *Por ejemplo, Matthieu Faou, Strategic Web compromises in the Middle East with a pinch of Candiru, WeLiveSecurity, 16 de noviembre de 2021; Hack Patrol, Getting Pegasus (NSO) False Positive. Vimeo, 7 de abril de 2022, https://vimeo.com/696991504*

*GitHub. Thehackpatrol/pegasus_false_positivo, 29 de abril de 2022 https://github.com/thehackpatrol/pegasus_false_positive*

*Testimonio de experto del profesor de informática Gregorio Martín (jubilado) en la Universidad de Valencia Parlamento Europeo, Centro Multimedia, Comisión de Investigación para investigar el uso del programa espía de vigilancia Pegasus y otros programas equivalentes, 28 de noviembre de 2022, https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20221129-0900-COMMITTEE-PEGA*

*Martín, Gregorio and Scott, Jonathan Scott (2023) CatalanGate Vectors: An Analysis of WhatsApp's Impact on Citizen Privacy and Amnesty International's MVT-Tool, Enero de 2023, https://www.researchgate.net/publication/367078083_CATALANGATE_VECTORS_An_Analysis_of_WhatsApp's_Impact_on_Citizen_Privacy_and_Amnesty_International's_MVT-_Tool*

73/

*GitHub. Jonathandata1/Pegasus-CatalanGate-False-Positives, 25 de noviembre de 2022*
*https://github.com/jonathandata1/Pegasus-CatalanGate-False-Positives*

74/

*Github AmnestyTech / investigations. Remove a file that creates false positive. 29 de julio de 2021,*
*https://github.com/AmnestyTech/investigations/commit/928ea5a820df6596762241da147b5afa1458b5ee*

*Github AmnestyTech / investigations. Removed indicator added by mistake, 29 de julio de 2021*
*https://github.com/AmnestyTech/investigations/commit/ad04b5473382faf860f595f2f2011a0ff2c19902*

*Github AmnestyTech / investigations. Warning + remove false positive, 22 de julio de 2021,*
*https://github.com/AmnestyTech/investigations/commit/ba749a926cec4bf43920c9300922296689fdc57b*

*Github AmnestyTech / investigations, removing false positive, 19 de julio de 2021*
*https://github.com/AmnestyTech/investigations/commit/1c694217c3efb4e40f34822b6ef99a7b5bd8a064*

75/

*Github AmnestyTech / investigations, Removing a dyndns base domain with hundreds of thousands of non-NSO users, 22 de julio de 2021*
*https://github.com/AmnestyTech/investigations/commit/ba0ec20fae598da83e875276ef82c7007241e822*

*Github AmnestyTech / investigations. Removed indicator added by mistake, 29 de julio de 2021,*
*https://github.com/AmnestyTech/investigations/commit/ad04b5473382faf860f595f2f2011a0ff2c19902*
*This last log shows 2 changed files with 14,932 additions and 14,981 deletions.*

76/

*Scott, J.B. (2022). Review of Catalangate Amnesty International Validation, 25 de noviembre de 2022, 10.13140/RG.2.2.10512.28160*
*https://www.researchgate.net/publication/365743925_Review_of_Catalangate_Amnesty_International_Validation*

La infalibilidad de los métodos de Citizen Lab reivindicada por el Sr. Deibert convencería a muy pocos científicos sociales rigurosos o expertos en ciencias sociales digitales. Su confianza en los métodos forenses de Citizen Lab contrasta con las concepciones generales de la ciencia y, en concreto, con las opiniones de expertos en el ámbito de la criminalística digital que reconocen los problemas de fiabilidad y que recomiendan las validaciones externas para reducir la posibilidad de errores causados por las herramientas de informática forense (algoritmos, aplicación o hardware), la metodología y la interpretación de los resultados (por ejemplo, Arshad *et al.* 2018; Horsman 2019; Hughes of Karabiyik 2020).[77] Aunque tanto el Sr. Deibert como el Sr. Scott-Railton tienen una formación disciplinaria en el ámbito de la ciencia política, llevan muchos años trabajando en el ámbito de la criminalística digital, por lo que deben ser conscientes de que los márgenes de error y los falsos positivos son una suposición común en este tipo de investigaciones. No parece adecuado que pretendan lo contrario en su investigación del CatalanGate — en la que personas con motivaciones políticas sin los conocimientos especializados adecuados manejaban pruebas y llevaron a cabo análisis preliminares—.

El 22 de diciembre de 2022, Citizen Lab admitió que había supuesto erróneamente que el Sr. Antoni Comín era una víctima de spyware debido a un error en el sistema de etiquetado que utilizaba durante el trabajo de campo[78]. Esto confirma los riesgos antes mencionados asociados a la atribución de la responsabilidad de la recogida de datos a personas sin experiencia en investigación o criminalística digital.

En 2017, el propio Sr. Deibert publicó un artículo en el que se cuestionaba un informe del DHS/FBI sobre el pirateo ruso para una serie de graves errores metodológicos que podrían ser igualmente aplicables al estudio CatalanGate. Por ejemplo, en 2017, Deibert cuestiona adecuadamente el denominado «Grizzled Steppe», al que califica de «decepcionante y contraproducente».

77/ *Arshad, H., Jantan, A. B., & Abiodun, O. I. (2018). Digital forensics: review of issues in scientific validation of digital evidence. Journal of Information Processing Systems, 14(2), 346-376; Horsman, G. (2019). Tool testing and reliability issues in the field of digital forensics. Digital Investigation, 28, 163-175; Hughes, N., & Karabiyik, U. (2020). Towards reliable digital forensics investigations through measurement science. Wiley Interdisciplinary Reviews: Forensic Science, 2(4), e1367.*

78/ *Ron Deibert (2022). CatalanGate Report Correcting a Case. 22 de diciembre de 2022, https://citizenlab.ca/2022/12/catalangate-report-correcting-a-case/*

Una de las críticas que formula es que:

«[u]n apéndice incluye una hoja de cálculo destinada a proporcionar *Indicadores de Compromiso*, listas largas de detalles técnicos supuestamente asociados a la campaña de espionaje. Entre ellas figuran las direcciones IP, las firmas de programas maliciosos y las infraestructuras de mando y control, que los defensores de la red deben utilizar para evitar el espionaje respaldado por Rusia, y que aparentemente se utilizarían para *tomar las huellas dactilares* de Rusia y tildarla de culpable. Lamentablemente, muchas de ellas están desfasadas o carecen de pertinencia, o se utilizan en múltiples campañas de ciberespionaje y no están asociadas exclusivamente a Rusia».[79]

79/

*Ronald Deibert (2017) The DHS/FBI Report on Russian Hacking was a Predictable Failure, Just Security, 4 de enero de 2017,*
*https://www.justsecurity.org/35989/dhsfbi-report-russian-hacking-predictable-failure/*

Así pues, el Sr. Deibert cuestionó la validez de utilizar determinados rastros o indicadores de compromiso (IOC) para acusar a Rusia, ya que estos también pueden ser utilizados por otros. Mientras tanto, el informe CatalanGate supone que ningún cibercriminal pensaría en utilizar mensajes institucionales españoles falsos, excepto los servicios secretos españoles, y que lo que consideran IOC de Pegasus no podrían ser empleados por otros fabricantes de programas espía o programas maliciosos. Se trata de una contradicción con la lógica utilizada anteriormente por el Sr. Deibert.

Del mismo modo, el Sr. Deibert afirmó en el mismo artículo que «es un perjuicio tanto para el público en general como para los investigadores expertos el no aclarar los grados de confianza asociados a cada indicador. Sin una categorización o un contexto adecuados, los indicadores no cumplen el objetivo de ayudar a los defensores de la red ni a demostrar la atribución». El informe CatalanGate no incluye ninguna evaluación de los grados de confianza de los IOC utilizados para detectar ataques e infecciones. En 2022, el informe CatalanGate incumple claramente las normas que uno de los autores y director de Citizen Lab defendía en 2017.

En el mismo artículo, el Sr. Deibert se queja de que «no hay ninguna fuente independiente de verificación» en relación con los informes de ciberseguridad y sugiere que «tenemos que incentivarles para que sean más transparentes en cuanto a los datos que pueden compartir con el público y más rigurosos en cuanto a lo que presentan para hacerlos útiles a los demás». La falta de transparencia mostrada por Citizen Lab en relación con su investigación en Cataluña entra en conflicto con los principios que su director defendió cinco años antes.

Como parte de una investigación similar en la India relativa a una solicitud del Tribunal Supremo de los EEUU, un comité técnico independiente examinó 29 teléfonos que, según Citizen Lab, fueron atacados con el programa espía Pegasus[80]. Este examen trató de investigar la veracidad de las acusaciones contra el Gobierno de la India de uso del programa espía Pegasus para atacar a activistas, periodistas, políticos, jueces

*80/* *Miles Kenyon (2020) Citizen Lab and Amnesty International Uncover Spyware Operation Against Indian Human Rights Defenders. Citizen Lab, 15 de junio de 2020* https://citizenlab.ca/2020/06/citizen-lab-amnesty-international-uncover-spyware-operation-against-indian-human-rights-defenders/

*81/* *The Times of India. 29 mobiles examined, malware found in 5, no conclusive proof of Pegasus: SC panel. 25 de agosto de 2022.* http://timesofindia.indiatimes.com/articleshow/93769955.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

*Newsclick. Justice Raveendran Committee Found no Conclusive Proof of Pegasus Use Against Dissidents: SC. 25 de agosto de 2022.* https://www.newsclick.in/Justice-RV-Raveendran-Committee-Found-Conclusive-Proof-Pegasus-Software-Against-Dissidents-Supreme-Court

y funcionarios gubernamentales. Sin embargo, el resultado del análisis puso de manifiesto que, de los 29 teléfonos examinados por el Comité Técnico, solo 5 tenían programas maliciosos, y que no era seguro que los programas maliciosos encontrados correspondieran a Pegasus.[81]

Además, Nadim Kobeissi[82], un conocido experto en análisis criptográficos y seguridad informática, también denuncia públicamente a Citizen Lab por «externalizar la «revisión *inter pares*» a amigos personales políticamente alineados, sobre la base de una evidencia falsificable y sin grupos de control»[83]. Además, afirma que «no solo es muy fácil, sino muy rentable, que existan programas maliciosos que adopten intencionadamente los patrones de comportamiento de Pegasus».[84] Kobeissi critica que Citizen Lab y Amnesty Tech estén construyendo acciones contra los gobiernos y atribuyendo ataques a Pegasus sobre la base de un pequeño subconjunto de URL en Internet cuyo propietario y gestión se desconocen.

El Sr. Deibert también advirtió en 2017 de que «las conclusiones basadas en creencias, pruebas parciales y filtraciones anónimas, no son un criterio para hacer políticas públicas informadas» Sin embargo, en una entrevista con El Confidencial, Ronald Deibert afirmó que «España es cliente de NSO, veremos más casos de dispositivos espiados», y basa este argumento en información filtrada (presuntamente) por empleados de NSO a Motherboard.[85]

Además, como indica el informe CatalanGate: «Aunque en la actualidad no atribuimos esta operación a entidades gubernamentales específicas, las pruebas circunstanciales sugieren un fuerte vínculo con el Gobierno de España, incluida la naturaleza de las víctimas y los objetivos, el calendario y el hecho de que España sea cliente gubernamental del grupo NSO».[86] Al parecer, en este caso, Citizen Lab está cometiendo todos los errores sobre los que su director y coautor del informe ha advertido en el pasado.

*82/* *Nadim Kobeissi*
*https://nadim.computer/*

*83/* *Nadim Kobeissi @kaepora, Twitter, 18 de julio de 2022,*
*https://twitter.com/kaepora/status/1549008104490164225?s=20&t=5eOMTc-7GNOLlTX1UdUb4Q*

*84/* *Nadim Kobeissi @kaepora, Twitter, 22 de julio de 2021*
*https://twitter.com/kaepora/status/1418146034014953474?s=20&t=kCeQvp_mja3tG7jJyRZv2w*

*85/* *El confidencial. Entrevista con el Director de Citizen Lab. Ronald Deibert: «España es cliente de NSO, Veremos más casos de móviles espiados». 2 de octubre de 2021.*

*86/* *Scott-Railton et al. CatalanGate página 2.*

Paradójicamente, en 2017 el Sr. Deibert afirmó que «las deficiencias del informe del DHS/FBI han dado lugar a resultados previsibles. El presidente electo Donald Trump y sus partidarios de la «veracidad» pueden seguir diseminando idioteces[87], como que «ningún ordenador es seguro». Esto es básicamente lo que ha ocurrido en España tras la publicación del informe CatalanGate, donde decenas de políticos y periodistas han replicado las acusaciones de Citizen Lab de espionaje «ilimitado, innecesario y desproporcionado» por parte del Gobierno español sobre la sociedad civil catalana y han difundido mensajes alarmistas similares cargados políticamente.[88] Por ejemplo, una página web creada por la organización secesionista Òmnium para denunciar el presunto espionaje de la sociedad civil catalana CatalanGate.cat tiene en su página de inicio el mensaje «CatalanGate: ens estan vigilant» (CatalanGate: nos están vigilando) y «CatalanGate: Democracy under surveillance» (Democracia bajo vigilancia) en la versión inglesa de la página web.[89] La organización secesionista Assemblea Nacional Catalana (ANC) creó una sección en su web con un vídeo dramático en el que se afirma, entre otras cosas: «Saben lo que dices, dónde vas, con quién te reúnes [...]. España, Hungría y Polonia son los únicos miembros de la UE que han espiado utilizando Pegasus. Países que han desafiado repetidamente el Estado de Derecho de la UE [...]. Denuncia la guerra sucia de España contra Cataluña»,[90]. El informe se ha instrumentalizado desde su publicación para promover un sentimiento de pánico moral en Cataluña y deslegitimar el Gobierno español a nivel internacional. El propio Sr. Deibert ha contribuido a ello haciendo públicas declaraciones alarmistas, como «esto tiene que ver con una agencia de espionaje que funciona sin control».[91]

87/ *Miles Kenyon (2020) Citizen Lab and Amnesty International Uncover Spyware Operation Against Indian Human Rights Defenders. Citizen Lab, 15 de junio de 2020*
*https://citizenlab.ca/2020/06/citizen-lab-amnesty-international-uncover-spyware-operation-against-indian-human-rights-defenders/*

88/ *The Times of India. 29 mobiles examined, malware found in 5, no conclusive proof of Pegasus: SC panel. 25 de agosto de 2022.*
*http://timesofindia.indiatimes.com/articleshow/93769955.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst*

89/ *Catalangate*
*https://catalangate.cat/*

90/ *#CatalanGate*
*https://assemblea.cat/catalangate-es/*

91/

*CCMA.cat. TV3. Pegasus, l'espia a la butxaca. 16 de octubre de 2022, https://www.ccma.cat/tv3/alacarta/30-minuts/pegasus-lespia-a-la-butxaca/*

# 5

# ¿Cuándo y dónde se realizaron los análisis forenses?

Citizen Lab se ha mostrado reacio a compartir información muy básica sobre cuándo, dónde y cómo se llevó a cabo la investigación «CatalanGate». Cuando se le preguntó sobre el calendario, el Sr. Deibert afirmó que «las actividades de divulgación e investigación comenzaron en otoño de 2019 y continuaron hasta el momento de su publicación» (18 de abril de 2022).[92] Esta cronología es problemática a distintos niveles. D. Roger Torrent, miembro del partido secesionista ERC y expresidente del Parlamento catalán, acusado por el Tribunal Constitucional de vulnerar los derechos de los diputados catalanes en la oposición[93] y que fue juzgado pero absuelto de cargos de desobediencia,[94] es identificado como el primer político secesionista catalán conocido públicamente como víctima de un ataque Pegasus por parte del informe CatalanGate.[95] Según el testimonio escrito del Sr. Roger Torrent, la investigación de su teléfono se inició a distancia a través de una red privada virtual (VPN) el 10 de julio de 2020 por el Sr. John Scott-Railton, que estaba en Toronto[96].

El Sr. Torrent menciona en su libro *Pegasus L'Estat ens espia* que el 21 de julio de 2020 se le dijo que: «Scott-Railton y Campo están trabajando en el informe final del caso en colaboración con una empresa estadounidense de comunicaciones».[97] Esto es muy sorprendente porque en ese momento todavía no se había confirmado ninguna infección mediante análisis forenses. También cabe destacar la referencia a la empresa estadounidense de comunicación, ya que sugiere que el informe estaba pensado desde el principio para ser instrumentalizado en una campaña de activismo político secesionista. ¿Colaboraron el Sr. Scott-Railton o el Sr. Campo con un grupo de interés profesional o una agencia o empresa de comunicación en julio de 2020 o en abril de 2022? Encaso afirmativo, ¿por qué y quién pagó por sus prestaciones?

*92/ Carta del Sr Ronald Deibert al Sr. Jordi Cañas, página 5.*

*93/* *VozPopuli. El Constitucional dice que Torrent vulneró los derechos de la oposición en el Parlament, 15 de noviembre de 2019*
*https://www.vozpopuli.com/espana/politica/torrent-derechos-oposicion-parlament-dui_0_1300670811.html*

*94/* *El Periódico. El Tribunal Superior absuelve a Roger Torrent del delito de desobediencia. 23 de noviembre de 2022*
*https://www.elperiodico.com/es/politica/20221123/mesa-parlament-torrent-desobediencia-constitucional-78936482*

*95/ Scott-Railton et al. (2022). Catalangate, página 3.*
*96/ Roger Torrent (2021). Pegasus: L'Estat que ens espia. Barcelona: Ara Llibres. Libro publicado en enero de 2021, páginas 37-39.*
*97/ Roger Torrent (2021). Pegasus, página 135.*

Aunque en la política y en la industria, el uso de los servicios de las empresas de comunicación profesionales es una práctica habitual, no es así en el mundo académico. Los costosos servicios de infografía (46.900 CAD) que la Escuela Munk de Asuntos Globales contrató a una empresa catalana simplemente para mejorar el impacto de los resultados del informe CatalanGate son extremadamente inusuales en el contexto de la investigación universitaria. No se ha encontrado ninguna página web de infografías tan sofisticadas en ninguno de los informes anteriores de Citizen Lab.[98]

El caso del presunto espionaje del Sr Torrent recibió una gran cobertura en los medios durante julio de 2020 y fue usada por los movimientos secesionistas para lanzar una campaña de comunicación internacional que involucró a Amnistía Internacional y al Comité de Derechos Humanos del Consejo de Europa. Sin embargo, esta temprana campaña de comunicación plantea algunas dudas, dado que, el 16 de julio de 2020, Citizen Lab informó al gabinete del Sr. Torrent de que el resultado del análisis remoto de su teléfono no mostraba ninguna infección en ese momento:

«Puedes confirmar al Presidente Torrent que, en este momento, su terminal telefónico no está infectado por ningún programa espía».[99]

El 27 de julio de 2020, ERC recibió notificación de que ninguno de los 9 teléfonos de políticos secesionistas catalanes y miembros de sus entornos cercanos, analizados a distancia desde Canadá y Estados Unidos por Citizen Lab, estaba infectado. El Sr. Torrent afirma:

*98/* *Publicaciones de Citizen Lab.*
*https://citizenlab.ca/publications/*

*Las costosas infografías mencionadas pueden consultarse en la siguiente dirección:*
*https://catalonia.citizenlab.ca/*

*99/* *Roger Torrent (2021). Pegasus, página 104.*

«Se nos han enviado las primeras conclusiones del seguimiento de los números de teléfono móvil que hemos transmitido a Citizen Lab: he transmitido a Marta la información que mi equipo me ha pasado. ¿Qué dicen? Por el momento no hay otros teléfonos móviles pirateados. Sin embargo, hemos identificado algunos SMS que son con seguridad ataques de Pegasus».[100]

Entonces, el 27 de julio de 2020, no había ningún caso de infección detectado. ERC esperaba conseguir la confirmación de algunos ataques para extender las demandas judiciales que, de todos modos, ya habían presentado. Hasta abril de 2022 no se anunciaron nuevos nombres y la denuncia judicial no se modificó para incluir nuevas víctimas presuntas. ¿Qué ocurrió entre esas fechas? Al parecer, o bien Citizen Lab no encontró ninguna infección en 2020 o decidieron ocultarla durante más de un año y medio. Pero ¿para qué guardar silencio si han encontrado otros casos y ya se ha presentado una reclamación judicial formalizada? Después de toda la atención prestada por los medios de comunicación en julio de 2020, no existe una explicación clara de la retención de pruebas forenses de presuntas violaciones de los derechos humanos durante tanto tiempo.

*100/ Roger Torrent (2021). Pegasus, páginas 142 y 151.*

Según el artículo de Ronan Farrow en The New Yorker, el teléfono del Sr. Jordi Solé fue analizado en marzo de 2022[101]. Más inusual es el caso del Sr. Jordi Sànchez. En una entrevista en vídeo[102] reconoce que realizaron algunas pruebas por teléfono cuando se encontraba en prisión, presuntamente en 2020 o antes, y que estas fueron negativas (es decir, no se detectó infección). No obstante:

«El Sr. Elies Campo y el equipo de Citizen Lab insistieron en revisar de nuevo mi teléfono móvil y el de mis familiares, y lo hicieron justo a principios de abril (2022), y en este segundo análisis descubrieron que había estado infectado».

Esto también sirve para arrojar algunas sombras sobre la validación llevada a cabo por Amnesty Tech. Si a principios de abril seguían comprobando llamadas telefónicas y descubriendo nuevas infecciones, ¿cuánto tiempo tuvo Amnesty Tech para validar las 4 muestras de infección que se les proporcionaron? Esto también es inusual, ya que, en teoría, Citizen Lab ya había recogido docenas de infecciones que podría haber enviado antes para su validación. Parece que, en la campaña de comunicación que se había coordinado con las organizaciones secesionistas, Ronan Farrow, y otras partes interesadas los obligaron a acelerar las fases finales de la investigación para que todo estuviera listo el 18 de abril de 2022.

Cuando se le preguntó sobre los análisis prospectivos y confirmatorios de los dispositivos de los políticos catalanes, el Sr. Deibert afirma que «para proteger la privacidad de los participantes en la investigación, no puedo facilitar información sobre dónde se llevó a cabo el análisis técnico del informe. Todos los análisis fueron validados por el Dr. Marczak»[103], lo que constituye una justificación muy inusual de la falta de transparencia en el informe CatalanGate sobre dónde se realizaron los análisis fo-

*101/ Ronan Farrow (2022). How Democracies Spy on their Citizens. The New Yorker, 25 de abril de 2022*

*102/* *Assemblea. Jordi Sànchez #CatalanGate. 26 de abril de 2022, https://youtu.be/9crBYexH6Ew. As the rest of the videos in this series, the presumed victim presents himself and claims "I have been spied illegally by the Spanish State for being an independence activist".*

*103/ Mr Ronald Deibert letter to Jordi Cañas página 4*

renses. Mencionar la ciudad o el laboratorio donde se analizaron los productos o especificar si el examen físico de los teléfonos formaba parte del problema no comprometería en modo alguno la privacidad de los participantes en la investigación.

El preámbulo de los Principios de Buena Gobernanza de la Universidad de Toronto hace referencia a «la necesidad de ser vista como responsable, a través de la transparencia, de cara a todas las partes interesadas y que apoyan a la Universidad».[104] La investigación y el informe de CatalanGate no parecen ajustarse a estas normas. ¿Por qué sería problemático revelar dónde se llevaron a cabo los análisis forenses desde el punto de vista de la privacidad de las presuntas víctimas? De hecho, parece que Citizen Lab no se siente cómodo admitiendo que no analizó físicamente (en persona, no de forma remota) ninguno de los teléfonos. El Sr. Roger Torrent explica en su libro que el examen de su teléfono solo se hizo a distancia desde Toronto, el 10 de julio, día en que el Sr. Scott-Railton le pidió que se conectara a una VPN.[105] ¿Se llevaron a cabo de forma remota los demás análisis del Sr. Scott-Railton, del Sr. Bill Marczak y del Sr. Bahr Abdul Razzak? ¿Viajó alguno de los 65 dispositivos a Canadá o a otros lugares para ser examinados físicamente/*in situ*?

Según la literatura académica, los análisis forenses exclusivamente digitales presentan muchas limitaciones y retos (por ejemplo, Kristennan *et al.* 2019; Montasari y *et al.* 2019; Yaacoub *et al.* 2021)[106], que sugieren la necesidad de complementarlos con analógicos no remotos. De los testimonios de los participantes parece desprenderse que los teléfonos nunca viajaron a Toronto y nunca fueron examinados físicamente por nadie que trabajase en Citizen Lab. El Sr. Campo puede haber examinado algunos de ellos físicamente, pero no formó parte del Citizen Lab hasta enero de 2022. Además, no era un especialista de criminalística digital. No hay pruebas de que ningún miembro de Citizen Lab hubiera viajado a Cataluña durante el trabajo de campo.[107]

*104/* *Consejo de Gobierno de la Universidad de Toronto (1991) Política de conducta ética en la investigación,* *https://governingcouncil.utoronto.ca/system/files/import-files/ppmar281991i4820.pdf*

*105/* *Roger Torrent (2021). Pegasus, página 37.*

*106/* *Krishnan, S., Zhou, B., An, MK (2019). Smartphone Forensic Challenges. International Journal of Computer Science and Security 13 (5), 183 – 200; Montasari, R., Hill, R., Carpenter, V., & Hosseinian-Far, A. (2019). The standardised digital forensic investigation process model (SDFIPM). In Blockchain and Clinical Trial (pp. 169-209). Springer, Cham.; Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). Digital forensics vs. Anti-digital forensics: Techniques, limitations and recommendations. arXiv preprint arXiv:2103.17028.*

*107/* *El Sr. Scott-Railton parece sugerir en abril de 2022 que no ha viajado a Barcelona. CCMA. TV3. Preguntes Freqüents. El Catalangate amb John Scott-Railton i Elies Campo, Lang Lang i Noemí Casquet* *https://www.ccma.cat/tv3/alacarta/preguntes-frequents/el-catalangate-amb-john-scott-railton-i-elies-campo-lang-lang-i-noemi-casquet/video/6155478/*

La Sra. Niamh Sweeney, antigua directora de Política Pública de WhatsApp, alegó lo siguiente en su declaración oficial a The Guardian de 28 de julio de 2020:

«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».[108]

Esta afirmación indica que WhatsApp no llevó a cabo un análisis forense exhaustivo del dispositivo del Sr. Torrent. Si Citizen Lab llegó a realizar un análisis forense exhaustivo sobre este teléfono, los resultados no se compartieron con WhatsApp, lo que también arroja algunas dudas sobre el tipo de colaboración que Citizen Lab y WhatsApp habían establecido en relación con la investigación de presuntas víctimas de Pegasus entre los clientes de la empresa estadounidense.

Citizen Lab afirma que:

«Nuestro análisis forense nos permite concluir con gran confianza que, de las 63 personas destinatarias de Pegasus, almenos 51 personas estaban infectadas».[109]

*108/* *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-target-of-2019-attack*

*109/* *Scott-Railton et al. (2022). Catalangate, página 5.*

Este número de personas coincide con la suma de las víctimas que figuran en la tabla de objetivos del apéndice, bien con una fecha aproximada de infección, bien con «[Incapaz de determinar la(s) fecha(s) específica(s) de infección(es)]».[110] Esto indica que Citizen Lab nunca encontró pruebas de infección en el teléfono del Sr. Torrent ni de ninguno de los demás líderes secesionistas que justificaron que el caso se convirtiera en un escándalo de prensa internacional en julio de 2020, lo que llevó a Citizen Lab a profundizar en este caso.

Por último, el Sr. Deibert explica en una declaración a Europa Press que el Sr. Campo fue contratado el 1 de febrero de 2022 para ayudar a identificar a posibles víctimas, para entrevistas y análisis, habiendo trabajado como voluntario desde julio de 2020.[111] Ello parece indicar que, en febrero de 2022, Citizen Lab no había encontrado pruebas suficientes para publicar un informe y, por lo tanto, necesitaba apoyo para encontrar más víctimas. Este enfoque es inusual en la investigación académica, a menos que se haya encargado una investigación o informe, algo que el Sr. Deibert se niega a admitir[112]. Sin embargo, parece coincidir con la versión de algunos de los participantes, que reconocieron que sus teléfonos se analizaron en la primavera de 2022. Citizen Lab sigue mostrando reticencia a confirmar cuántas de las 65 víctimas fueron contactadas y sus dispositivos analizados en 2020, 2021 y 2022. Esta omisión podría interpretarse como un intento de ocultar un calendario problemático en la investigación que podría indicar interferencias de agentes e intereses ajenos a las normas de conducta académica previstas.

*110/ Scott-Railton et al. (2022). Catalangate, páginas 26-34.*

*111/* *Assemblea. Jordi Sànchez #CatalanGate. 26 de abril de 2022, https://youtu.be/9crBYexH6Ew. Como en el resto de los vídeos de esta serie, la presunta víctima se presenta y afirma que «el Estado español me ha espiado ilegalmente por ser un activista de la independencia».*

*112/ Carta del Sr.Ronald Deibert a Jordi Cañas, página 4*

# 6

# Conflicto de intereses y confiar el trabajo de campo a un activista político sin experiencia previa

La divulgación de posibles conflictos de intereses se espera en cualquier trabajo académico. El informe CatalanGate fue publicado por el Citizen Lab de la Universidad de Toronto, por lo que se supone que se adhiera a las normas académicas y que sigue las consideraciones éticas de la investigación. El Sr. Deibert confirmó que «la publicación de conflictos de intereses forma parte de los protocolos éticos de investigación de la Universidad de Toronto»[113]. Sin embargo, este informe no incluye ninguna declaración que reconozca (o rechace) conflictos de intereses por parte de los autores o de quienes colaboran en la investigación. El trabajo de campo fue coordinado por un activista a favor de la independencia y una presunta víctima del espionaje, sin experiencia previa en investigación ni título de enseñanza superior: el Sr. Elias Campo. Este autor también hizo afirmaciones falsas sobre su situación laboral y no fue miembro de Citizen Lab durante la mayor parte del período de investigación.

Aunque el informe CatalanGate menciona al Sr. Campo como empleado de Telegram, y también lo incluye en su perfil de LinkedIn entre septiembre de 2015 y diciembre de 2021,[114] Telegram ha rechazado formalmente esta alegación en dos ocasiones. La primera vez, Telegram emitió una declaración tras una entrevista muy controvertida con el Sr. Elies Campo en Wired. Esta se publicó poco después de convertirse en *fellow* del Citizen Lab. En ella, el Sr. Campo se presentó como «jefe de crecimiento, negocio y colaboraciones de Telegram» y afirmó que el Sr. Pavel Durov, director general de Telegram, había ignorado en gran medida su consejo sobre la actividad de la extrema derecha en la plataforma.[115]

*113/ Carta del Sr. Ronald Deibert al Sr. Jordi Cañas, página 6.*

*114/* *LinkedIn. Elies Campo.*
*https://www.linkedin.com/in/eliescampo*

*115/* *Wired. How Telegram Became the Anti-Facebook.*
*8 de febrero de 2022*
*https://www.wired.com/story/how-telegram-became-anti-facebook/*

«Elyes [sic] Campo nunca ha trabajado para Telegram, ni mucho menos liderado nada. En 2016, estaba realizando labores como voluntario y recibió una dirección de correo electrónico temporal, que fue posteriormente revocada. Nunca recibió ninguna compensación económica de Telegram y no firmó ningún contrato con nosotros. Las conversaciones con Pavel Durov, a las que hace referencia en el artículo, nunca tuvieron lugar».[116]

**Servicio de Prensa de Telegram**

Tras la publicación del informe «CatalanGate», el periódico español El Triangle se puso en contacto con Telegram, que dio una respuesta similar:

«Mr Elies Campo nunca ha sido empleado por Telegram en ningún cargo, ni mucho menos como responsable de nada».[117]

**Remi Vaughn**
*Representante de Telegram*

116/ *The Times Hub. Who is Elies Campo: Telegram officially commented on the scandalous interview with Wired. 11 de febrero de 2022, https://web.archive.org/web/20220401024159/https://thetimeshub.in/who-is-elies-campo-telegram-officially-commented-on-the-scandalous-interview-with-wired*

117/ *El Triangle. Elies Campo ha enganyat Citizenlab i 'The New Yorker'. 6 de mayo de 2022, https://www.eltriangle.eu/2022/05/06/elies-campo-ha-enganyat-citizenlab-i-the-new-yorker/*

Sin embargo, parece que esta no fue la primera vez que el Sr. Campo afirmó falsamente trabajar para una empresa. En una entrevista con La Vanguardia en 2014, el Sr. Campo admitió que se había reunido con gobiernos, operadores y periodistas pretendiendo ser un empleado de WhatsApp, antes de ser contratado.[118] Parece extraño que una institución académica confiara a un voluntario con intereses personales en un proyecto tan delicado, sin realizar ninguna comprobación de antecedentes.

El Sr. Campo participó abiertamente en la organización del referéndum ilegal de independencia en Cataluña en 2017, como demostró en sus redes sociales: por ejemplo, llevó una urna a un «colegio electoral»; también compartió la cuenta Tsunami Democràtic de Telegram[119]. Cabe recordar que muchas de las movilizaciones promovidas por el Tsunami Democràtic provocaron violencia y costaron millones de euros en daños. Entre el 14 y el 20 de octubre de 2019 se detectaron 534 incidentes violentos.[120]

*118/* *La Vanguardia. Elies Campo: "No siento presión por ocupar el primer cargo internacional en WhatsApp". 28 de febrero de 2014, https://www.lavanguardia.com/vida/20140228/54402684723/elies-campo-no-siento-presion-ser-primer-no-norteamericano-trabajar-whatsapp.html*

*119/* *Elies Campo. @elies. Twitter. 1 de abril de 2018: https://twitter.com/elies/status/980560731518091264?-t=m9yx1C2wBSGTz15Zjvbk8g&s=09*

*Elies Campo. @elies. Twitter. 29 de julio de 2019. https://twitter.com/elies/status/1023473276079628289?s=20&t=gKQOHs93qCfOpu0Ii-0Qfew*

*Elies Campo. @elies. Twitter. 7 de octubre de 2019. https://twitter.com/elies/status/1181216299168550914?s=20&t=gK-QOHs93qCfOpu0Ii0Qfew*

*Elies Campo. @elies. Twitter. 8 de noviembre de 2017, https://twitter.com/elies/status/928152272097263616?s=20&t=gK-QOHs93qCfOpu0Ii0Qfew. Cabe señalar que la plataforma Tsunami Democràtic se utilizó para coordinar muchos actos ilícitos de sabotaje y bloqueo y que la justicia española la está investigando.*

*120/* *El Confidencial. Violencia política en Cataluña: Casi 1.000 acuerdos en el último semestre de 2019. 7 de mayo de 2020, https://www.elconfidencial.com/espana/cataluna/2020-05-07/violencia-politica-en-cataluna-1000-agresiones-ultimo-semestre_2583619/*

También participó en la iniciativa Vocdoni, junto con otras presuntas víctimas de la investigación, como el Sr. Xavier Vives, el Sr. Pau Escrich y el Sr. Baylina.[121] Esta iniciativa, supuestamente confirmada por el movimiento catalán de independencia, utilizó la tecnología de blockchain Ethereum para crear sistemas de votación fuera del control del Gobierno español y facilitar así la creación de una República Catalana.[122] Vocdoni fue creado en Estonia con una estructura opaca en la que participan seis empresas y ocho empleados, y con prácticas anormales de facturación.[123]

*121/* *CoinDesk. Aragon Acquires Voting Project Vocdoni to Flesh Out Decentralized Governance Stack. 11 de enero de 2021, https://www.coindesk.com/tech/2021/01/11/aragon-acquires-voting-project-vocdoni-to-flesh-out-decentralized-governance-stack/*

*Vocdoni Blockchain Voting. @vocdoni. Twitter. 13 de febrero de 2022,https://twitter.com/vocdoni/status/1492859854897229826?s=20&t=FuM2Am-3iBckW1f4OBWh8g*

*Vocdoni Blockchain Voting. @vocdoni. Twitter. 13 de marzo de 2022, https://twitter.com/vocdoni/status/1503142345063161867?s=20&t=FuM2Am-3iBckW1f4OBWh8g*

*Xavivives.com. Xavi capactions. https://xavivives.com/#?expr=[%22i12D3KooWBSEYV1cK821KKdfVTHZc3gKaGkCQXjgoQotUDVYAxr3clzfmhs7a%22,[[%22i12D3KooWBSEYV1cK821KKdfVTHZc3gKaGkCQXjgoQotUDVYAxr3c2lf4dbua%22,%22i12D3KooWBSEYV1cK821KKdfVTHZc3gKaGkCQXjgoQotUDVYAxr3cwx4lcc2a%22],[%22i12D3KooWBSEYV1cK821KKdfVTHZc3gKaGkCQXjgoQotUDVYAxr3c2lf4dbua%22,%22i12D3KooWBSEYV1cK821KKdfVTHZc3gKaGkCQXjgoQotUDVYAxr3cclw35kma%22]]]&*

*122/* *El Confidencial. Los ingenieros de Tsunami Democràtic crearon una 'app' de voto para un nuevo referéndum. 29 de abril de 2022, https://www.elconfidencial.com/espana/2022-04-29/pegasus-espionaje-cni-tsunami-democratic-vocdoni-referendum_3416269/*

*123/* *El Confidencial. La Guardia Civil ubica a Soros tras una 'app' para blindar un nuevo referéndum en Cataluña. 25 de octubre de 2022, https://www.elconfidencial.com/espana/2022-10-25/guardia-civil-ubica-soros-app-blindar-nuevo-referendum-cataluna_3511853/*

**Elies Campo**
@elies

6 months ago today, I had the honor of bringing a ballot box into the polling station for the Catalan Independence Referendum. **#CatalanReferendum #Ref1Oct**
Thank you **@catalan_gov!**

**#freePuigdemont**
**#FreeCatalanPoliticalPrisoners**
**#LlibertatPresosPolítics**

11:41 PM · 1 de abril, 2018

**Elies Campo**
@elies

General Strike starting to be in full effect in #Catalonia as main access highways to Barcelona are blocked. #VagaGeneral

> **CDR Sant Andreu** @CDRstap · Nov 8, 2017
>
> Ronda tallada pels 2 sentits al nus de la Trinitat. Molta tensió.

8 de noviembre, 2017

**Elies Campo**
@elies

As we end the **@AspenAction** Forum on Fearless Leadership, Aspen fellows show support and demand justice and freedom for Catalonia's political prisoners. **#AspenAction**

**#FreeCatalanPoliticalPrisoners**

29 de julio, 2018

**Elies Campo**
@elies

El canal de **@tsunami_dem** a **@Telegram** ha sobrepassat els 76000 subscriptors. Més de l'1% de la població de Catalunya. Possiblement el canal públic en català amb més subscriptors a Telegram.

**t.me/tsunamid**

4:34 PM · 7 de octubre, 2019

El Sr. Campo formó parte de un equipo de 30 asesores cuando el entonces Presidente de la Generalitat, Joaquim Torra, puso en marcha, el 2 de junio de 2020, la estrategia «Catalunya 2022, Reset, Crida per reactivar el país»[124]. La policía inició una investigación sobre los esfuerzos por crear una República Digital Catalana para facilitar su separación de España.[125]

**Vocdoni Blockchain Voting | We're hiring..** ···
@vocdoni

Replying to **@0x5adb07 @joseolivas** and **3 others**

Because of course paper ballots are notoriously safe and secure in Spain. **counterfire.org/articles/opini...**

3:59 · 22 Dec 2017

**Vocdoni Blockchain Voting...** @vocdoni · Mar 13, 22

Fantastic news! **@Òmnium**, the largest cultural non-profit in **#Catalonia**, with aprox 200k members, used Vocdoni for its Board of Director **#elections** at its 2022 AGM. We are proud to celebrate democracy by providing **#blockchain** voting such a prestigious institution [1/2]

**Vocdoni Blockchain Voting...** @vocdoni · Mar 13, 22

For the 4th year in a row, Vocdoni processed all 21,758 votes cast. Founded in 1961, Òmnium Cultural reflects the strong democratic & decentralist political culture of Catalonia. We know **#blockchaintechnology** will continue to empower individual sovereignty in the future. [2/3]

**Vocdoni Blockchain Voting | We're hiring..** ···
@vocdoni

Congratulations to the **@Òmnium_26** candidacy for winning their election to the board! [3/3]

3:59 · 22 Dec 2017

*124/* *GenCat. Catalunya 2022. https://presidencia.gencat.cat/ca/ambits_d_actuacio/catalunya-2022/. El Sr. Campo también se reunió anteriormente con el Sr. Torra durante una visita oficial a los EE.UU.*

*125/* *El Español. El ingeniero que denunció el espionaje con Pegasus a separatistas desarrolló la República Digital Catalana. 25 de octubre de 2022, https://www.elespanol.com/espana/20221025/ingeniero-pegasus-separatistas-desarrollo-republica-digital-catalana/713179083_0.html*

Además, el Sr. Campo también conocía personalmente a varios de los demás actores implicados en el esfuerzo por lograr la independencia unilateral catalana. Viajó varias veces a Bélgica para visitar al Sr. Carles Puigdemont, antiguo presidente de la Generalitat Cataluña, que pese a una orden de detención internacional se escapó de la justicia.[126] ¿Expresó alguien de Citizen Lab su consternación por conceder un papel clave, como el de la tramitación de pruebas, a un activista implicado en un intento de secesión contra una democracia europea? ¿Expresó alguien de Citizen Lab su preocupación por posibles conflictos de interés por parte del Sr. Campo, dado que era un activista partidario de la independencia y conocido de muchas de las presuntas víctimas que estaban surgiendo?

Cuando se le preguntó al Sr. Deibert: «cuando Citizen Lab le confió el trabajo de campo al Sr. Elies Campo, ¿sabían ya que estaba siendo monitorizado por los servicios de inteligencia españoles por su supuesta implicación en varias actividades secesionistas ilegales?», este afirmó que «Citizen Lab no tuvo conocimiento de las acusaciones formuladas contra el Sr. Campo hasta después de la publicación del informe». Sin embargo, no parece creíble que Citizen Lab ignorara su implicación, dado que el propio Sr. Campo aparece como presunta víctima de espionaje en el informe que sugiere que Pegasus estaba siendo utilizado por España para supervisar a políticos y activistas, precisamente por su implicación en las actividades secesionistas.

Citizen Lab no ha explicado cuándo ni cómo descubrió que el teléfono del Sr. Campo había sido atacado por programas espía. Tampoco parecían expresar su preocupación por la posible implicación del Sr. Campo en actividades ilícitas o ilegales que podrían haber motivado el presunto espionaje por parte de las fuerzas de seguridad españolas. Una vez más, parece que la única hipótesis de Citizen Lab era la de investigaciones «ilegales» por parte del gobierno.

El Sr. Deibert explica la distribución del trabajo para el informe, asignando al Sr. Campo la responsabilidad de coordinar el acercamiento a otras presuntas víctimas. Al mismo tiempo, el informe señala lo siguiente: «... Citizen Lab, en colaboración con organizaciones de la sociedad civil, llevó a cabo una gran investigación sobre el *hacking* de Pegasus en España». ¿Ha manifestado algún miembro del equipo su preocupación por el posible sesgo de selección debido a la responsabilidad del Sr. Campo en la selección de los casos?

*126/* *El Mundo. La Guardia Civil 'cazó' al autor del 'informe Pegasus' en Bruselas con Puigdemont. 29 de abril de 2022, https://www.elmundo.es/espana/2022/04/29/626c3e96e4d4d8bb1c8b4597.html*

*Crónica Global. El 'cerebro' del Catalangate visitó a Puigdemont en Bélgica, 30 de abril de 2022, https://cronicaglobal.elespanol.com/politica/cerebro-catalangate-puigdemont-belgica_655106_102.html*

Al preguntar si el Sr. Elies Campo había revelado cualquier conflicto de intereses a la Comisión de Investigación Ética de la Universidad de Toronto, el Sr. Deibert respondió que no había conflicto de intereses planteado por el trabajo del Sr. Elies Campo con Citizen Lab, y que el Sr. Campo actuó bajo su supervisión y autoridad y que «no trabajó de manera independiente».[127] Además, de la declaración del Sr. Deibert y de los intercambios con la Universidad de Toronto, se puede inferir que no se solicitaron u otorgaron permisos específicos en relación con la investigación en Cataluña, y que el Consejo de Ética no fue informado de que los partidos políticos (y sus abogados) estaban detrás de los análisis forenses y la selección de casos para el informe, mientras planeaban usar la evidencia en los tribunales.

Parece, pues, que el Consejo de Ética de la Investigación Universitaria (REB) hubiese dado «carta blanca» a Citizen Lab en relación con el proyecto Pegasus.

El Sr. Deibert afirma que la divulgación en Cataluña fue supervisada por él mismo y que el Sr. Campo «no trabajó de forma independiente». Sin embargo, no hay pruebas de que ningún miembro de Citizen Lab viajara regularmente a Cataluña entre julio de 2020 y abril de 2022 para supervisar el trabajo del Sr. Campo, que no tuvo afiliación formal a Citizen Lab hasta febrero de 2022.[128] ¿Por qué no se le concedió la condición de *fellow* en 2020, cuando comenzó su trabajo para Citizen Lab si era el coordinador de la investigación y debía estar vinculado por los protocolos de ética de la investigación de la Universidad de Toronto? Además, según la información revelada en una solicitud a la Oficina de Libertad de Información y Protección de la Privacidad (FIPPA), la Universidad de Toronto no encontró actas de las reuniones relativas a la investigación de CatalanGate de Citizen Lab.

Presumiblemente, el Sr. Campo no había completado ningún título universitario y no tenía experiencia en la investigación científica. Por lo tanto, debería haber recibido cierta formación formal en materia de criminalística digital y de ética en la in-

*127/ Carta del Sr. Ronald Deibert al Sr. Jordi Cañas, página 3.*

*128/* *El perfil LinkedIn de Elies Campo afirma que es colaborador en Citizen Lab desde enero de 2022, aunque el Sr. Deibert especifica que fue contratado el 1 de febrero de 2022 para ayudar a identificar posibles víctimas, para entrevistas y análisis. Europa Press. El director de The Citizen Lab justifica que Elies Campo investigue en un caso en el que también fue objetivo de espionaje. 8 de mayo de 2022,, https://www.europapress.es/nacional/noticia-director-the-citizen-lab-justifica-elies-campo-investigue-caso-tambien-fue-objeto-espionaje-20220508101651.html*

*En una entrevista en TV3, el Sr. Campo explica cuándo comenzó a coordinar la segunda fase de la investigación. CCMA. TV3. Preguntes Freqüentes. El Catalangate amb John Scott-Railton i Elies Campo, Lang Lang i Noemí Casquet https://www.ccma.cat/tv3/alacarta/preguntes-frequents/el-catalangate-amb-john-scott-railton-i-elies-campo-lang-lang-i-noemi-casquet/video/6155478/*

vestigación antes de que se le asignara la tarea de coordinar la divulgación. No hay pruebas de que se le ofreciera dicha formación.

Cuando se le preguntó qué tipo de conocimientos especializados o capacidades sirvieron para elegir al Sr. Elies Campo como coordinador del trabajo de campo en Cataluña, Deibert, respondió que «Citizen Lab trabaja regularmente con personas que gozan de confianza en las comunidades objeto del uso de Pegasus para contactar y ayudar a coordinar el acercamiento a los grupos de alto riesgo. No se requieren conocimientos técnicos especiales para esta especialidad».[129] Sin embargo, como muestran los testimonios de muchos participantes en la investigación, Campo fue la persona que realizó muchos de los análisis forenses. La toma de muestras y el acercamiento en el contexto de una investigación muy sensible, en la que participaron personas investigadas por la actividad criminal en una democracia (España ocupó el puesto 9 en el mundo por el prestigioso índice democrático de V-Dem en 2020)[130] requiere una comprensión tanto de la metodología como de la ética de la investigación.

El Sr. Deibert no responde plenamente a las preguntas sobre el momento del primer contacto del Sr. Elies Campo con Citizen Lab, ni a cuándo confió en el trabajo de campo en Cataluña; simplemente reconoció que «el Sr. Campo se puso en contacto por primera vez con el Citizen Lab en 2020» y que prestó «asistencia de acercamiento a Citizen Lab entre 2020 y 2022»[131] En una entrevista televisiva, el Sr. Campo afirmó que, en octubre de 2019, WhatsApp y Citizen Lab enviaron notificaciones a posibles víctimas de una presunta violación de la seguridad en WhatsApp, y que algunas de estas presuntas víctimas, sabiendo que había trabajado para WhatsApp, se pusieron en contacto con él para pedirle que consiguiera más información sobre la veracidad de esos ataques. El Sr. Campo afirma que llamó a sus antiguos colegas de WhatsApp, quienes confirmaron que los mensajes eran auténticos y que debería ponerse en contacto con Citizen Lab para obtener más información.

*129/ Carta del Sr. Ronald Deibert al Sr. Jordi Cañas, páginas 3 y 5.*

*130/* *Coppedge, Michael, John Gerring, Carl Henrik Knutsen, Staffan I. Lindberg, Jan Teorell, Nazifa Alizada, David Altman, Michael Bernhard, Agnes Cornell, M. Steven Fish, Lisa Gastaldi, Haakon Gjerløw, Adam Glynn, Allen Hicken, Garry Hindle, Nina Ilchenko, Joshua Krusell, Anna Lührmann, Seraphine F. Maerz, Kyle L. Marquardt, Kelly McMann, Valeriya Mechkova, Juraj Medzihorsky, Pamela Paxton, Daniel Pemstein, Josefine Pernes, Johannes von Römer, Brigitte Seim, Rachel Sigman, Svend-Erik Skaaning, Jeffrey Staton, Aksel Sundström, Eitan Tzelgov, Yi-ting Wang, Tore Wig, Steven Wilson and Daniel Ziblatt. (2021). V-Dem [Country–Year/Country–Date] Dataset v11.1. Varieties of Democracy (V-Dem) Project.* https://doi.org/10.23696/vdemds21.

*131/ Ronald Deibert al Sr. Jordi Cañas página 5.*

El relato del Sr. Campo sobre las razones por las que descubrió Pegasus y cómo ofreció sus servicios a Citizen Lab plantea varias dudas. Resulta sorprendente que nadie en Citizen Lab haya manifestado su preocupación por los posibles conflictos de intereses del Sr. Campo, dado que se presentó como empleado de Telegram y Citizen Lab, en teoría, ayudó a WhatsApp (competidor de Telegram) a llegar a posibles víctimas. Además, la historia del Sr. Campo sobre cómo había sido incorporado al caso también debería haber suscitado preocupación en Citizen Lab. Presumiblemente, el Sr. Campo trabajó en WhatsApp entre 2013 y 2014.[132] Afirmó que «quería trabajar para WhatsApp y no esperaba a recibir una oferta, sino que crearía su propio trabajo».[133] El Sr. Campo abandonó la empresa una vez que Facebook la compró, cuando manifestó públicamente que Facebook era «el mayor fraude jamás creado» y que la integración de WhatsApp en esta empresa era peligrosa y «traicionaba» los valores del usuario.[134] Es sorprendente que alguien que había expresado críticas tan contundentes pudiese volver a su empresa y solicitar información interna a antiguos compañeros, algo que se espera que los acuerdos de confidencialidad de *Big Techs* eviten.

El artículo del Sr. Ronan Farrow en The New Yorker y el informe de CatalanGate se refieren a una acción polémica y potencialmente ilegal del Sr. Campo durante la investigación. El informe reconoce que «Citizen Lab ayudó a Whatsapp a notificar a las víctimas de la sociedad civil y ayudarlas a tomar medidas para protegerse»[135].

El Sr. Farrow explica que en febrero de 2021, Citizen Lab identificó una infección activa en un ordenador portátil perteneciente al Sr. Joan Matamala, que era uno de los 18 líderes a los que monotorizarion los servicios secretos españoles con autorización judicial[136], según el Defensor del Pueblo español[137]:

*132/* *Elies Campo. LinkedIn.* *https://www.linkedin.com/in/eliescampo/*

*133/* *El Confidencial. "Quería trabajar para WhatsApp y no esperé a una oferta, sino que creé mi puesto". 17 de diciembre de 2014,* *https://www.elconfidencial.com/tecnologia/2014-12-17/queria-trabajar-para-whatsapp-y-no-espere-a-una-oferta-sino-que-cree-mi-puesto_592226/*

*134/* *El Confidencial. El español que dejó su trabajo en WhatsApp: "Facebook es la mayor estafa jamás creada". 2 de enero de 2017,* *https://www.elconfidencial.com/tecnologia/2017-01-02/whatsapp-facebook-elies-campo_1310536/*

*135/* *Scott-Railton et al. (2022). CatalanGate, página 1.*

*136/* *La Vanguardia. 14 de mayo de 2022. Els 18 espiats pel CNI,* *https://www.lavanguardia.com/encatala/20220514/8266154/els-18-espiats-pel-cni.html*

# «El Sr. Campo llamó a Matamala y le dio instrucciones para envolver el ordenador portátil en papel de aluminio, una forma improvisada de impedir que los programas maliciosos se comunicaran con servidores».[138]

**Ronan Farrow**
*New Yorker*

Esta versión, que el Sr. Campo confirma en una entrevista en TV3,[139] podría interpretarse como un esfuerzo activo para obstaculizar una investigación judicial española. Esta obstrucción de la justicia de un estado democrático durante el trabajo de campo debería suponer lógicamente una violación de los protocolos éticos de investigación en la Universidad de Toronto en cualquier otra institución académica seria.

137/ *El País. El Defensor avala las 18 escuchas con Pegasus admitidas por el CNI, pero pide un mejor control judicial. 18 de mayo de 2022, https://elpais.com/espana/2022-05-18/el-defensor-avala-las-18-escuchas-con-pegasus-admitidas-por-el-cni-pero-pide-un-mejor-control-judicial.html*

138/ *Ronan Farrow (2022). How Democracies Spy on their Citizens. The New Yorker, 25 de abril de 2022 https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens*

*Aunque no se reconoce en el informe CatalanGate, el informe Hooking Candiru especifica que la primera infección de Candiru, que se supone que corresponde a la del Sr. Matamala, se localizó utilizando datos de telemetría del Team Cymru. Mar Zack et al. (2021). https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/*

139/ *CCMA.Cat. TV3. Preguntes Freqüents. El Catalangate amb John Scott-Railton i Elies Campo, Lang Lang i Noemí Casquet, 23 de abril de 2022; https://www.ccma.cat/tv3/alacarta/preguntes-frequents/el-catalangate-amb-john-scott-railton-i-elies-campo-lang-lang-i-noemi-casquet/video/6155478/*

Desde julio de 2020, Citizen Lab ha venido sugiriendo públicamente que es probable que los servicios de seguridad de España lleven a cabo ataques con programas espía en Cataluña. ¿Alguien de Citizen Lab expresó alguna preocupación por la posible interferencia de su trabajo de campo en el curso de la justicia española? ¿Autorizó la Universidad de Toronto a Citizen Lab para ayudar a prevenir ataques con programas espía contra personas que fueron investigadas posteriormente por los tribunales españoles y las fuerzas policiales? Una autorización genérica para investigar a Pegasus en regímenes autoritarios, en los que no se aplica el Estado de Derecho, difícilmente debería ser suficiente para cubrir este tipo de actividades de investigación en las democracias. Por desgracia, parece que estas decisiones de investigación sumamente complejas en el caso de la investigación CatalanGate se realizaron sin autorización formal de la Universidad de Toronto o de su Consejo de Ética de la Investigación.

Además, cabe señalar que la implicación de los partidos secesionistas en la investigación implica algunas consideraciones éticas de investigación que tampoco fueron mencionadas por Citizen Lab. Según varios testimonios, los partidos y organizaciones políticos favorables al secesionismo participaron directamente en la realización de análisis técnicos en los teléfonos de las presuntas víctimas que aparecen en el informe CatalanGate[140], lo que resulta muy problemático, ya que Citizen Lab no reconoce este conflicto de intereses. Según el libro del Sr. Torrent, ERC creó un equipo, el 9 de julio de 2020, que trabajó en una investigación de Pegasus paralela a la de Citizen Lab.[141] Solo después de la visita del Sr. Torrent al Sr. Oriol Junqueras (antiguo líder de ERC) en la prisión de Lledoners, el 10 de julio de 2020, autorizó a Citizen Lab a investigar su teléfono.

## «Escucho la voz de Romeva que les grita: ¡Vamos hasta el fondo del asunto! Y la de Junqueras: No dejes que esto ocurra, ¡denúncialo!».[142]

*140/* *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*

*Torrent (2021) Pegasus. p. 142; Parlamento Europeo, Centro Multimedios, Comisión de Investigación para investigar el uso del programa espía de vigilancia Pegasus y otros programas equivalentes, 28 de noviembre de 2022, https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20221129-0900-COMMITTEE-PEGA*

*141/ Roger Torrent (2021). Pegasus, páginas 31-32.*
*142/ Roger Torrent (2021). Pegasus, páginas 36-37.*

El Sr. Torrent invitó inmediatamente al periodista Jordi Basté a la reunión con el Sr Junqueras con quién se entrevistó el 15 de julio y presentó al Sr. Elies Campo al Sr. Torrent en directo.[143] Cabe señalar que en ese momento no se había realizado ningún análisis forense y que probablemente los otros 4 políticos y activistas secesionistas de la lista de presuntas víctimas de WhatsApp habían sido notificados antes. Como tal, se ha alegado que la verdadera razón de la decisión de investigar a Pegasus en julio de 2020 y no en octubre de 2019 fue el oportunismo político[144].

El Sr. Torrent alega que Oriol Sagrera — su jefe de gabinete — estaba recopilando mensajes SMS sospechosos para transmitirlos a los Sres. Scott-Railton y Campo:

«Ahora que sabemos de qué va todo esto, casi no necesitamos científicos informáticos para discernir mensajes sospechosos de otros inofensivos. Nos hemos convertido en rastreadores expertos [...] Estamos contando y recopilando toda la infromación para transmitirla a Elies Campo. En el caso de JxCat, están haciendo lo mismo. Boye está realizando un inventario».[145]

El informe no reconoce si Citizen Lab era consciente de que ERC y JxCat contaban con un equipo que llevaba a cabo una investigación paralela de Pegasus y seleccionaba los casos que transmitieron a los Sres. Campo y Scott-Railton. Cualquier investigación científica seria consideraría que se trata de una interferencia en la metodología de muestreo de bola de nieve seguida

*143/ Roger Torrent (2021). Pegasus, páginas 37 y 76.*

*144/* *Ms Anaïs Franquesa a lawyer and activist at Òmnium suggests that ERC politicians knew about the presumed espionage months before but timing was decided for political considerations. Youtube. Canòdrom Ateneu d'Innovació Digital i Democràtica. A l'ombra de Pegasus | Drets civils en l'era de la vigilancia. 3 de noviembre de 2022. Min 49:35, https://www.youtube.com/watch?app=desktop&v=OcFBZBIWttY&feature=emb_imp_woyt*

*145/ Roger Torrent (2021). Pegasus, página 143. Se refiere a to 24 de julio de 2020.*

por Citizen Lab. Es poco probable que el Consejo de Ética de Investigación fuera consciente de la implicación directa de estos activistas políticos en los análisis técnicos, y el propio Sr. Deibert lo negó en una declaración pública.

## «Ningún partido político catalán ni organización secesionista participó en la redacción del informe ni en el análisis técnico realizado por Citizen Lab para este informe».[146]

**Sr Deibert**

Los políticos y activistas secesionistas que analizan los teléfonos tenían un interés real en maximizar el número de infecciones y ataques encontrados y también podrían haber sesgado la muestra por sus propios intereses intrínsecos o partidistas, aunque todos los teléfonos analizados pertenecían a políticos y activistas favorables a la independencia, cada uno de los partidos y organizaciones tenía sus propios intereses. Muchos de los activistas, como los Sres. Sergi Miquel, Baylina, Escrich, Ganyet y Vives, eran activistas secesionistas con conocimientos informáticos avanzados, podrían incluso haber alterado potencialmente las pruebas. El informe debería haber reconocido explícitamente esta debilidad en relación con la cadena de custodia de las pruebas, al tiempo quese planteaban las siguientes preguntas:

A → *Además del Sr. Campo, ¿quiénes eran los demás activistas y políticos partidarios de la independencia que participaron en los análisis técnicos realizados en esta investigación (incluido el análisis técnico preliminar para los casos de preselección enviados a Toronto)?*

B → *Además del Sr. Campo, ¿participaron en la redacción del informe otros activistas y políticos partidarios de la independencia?*

C → *¿Se implicó a partidos políticos secesionistas catalanes o las organizaciones secesionistas en la definición del calendario del proyecto y la estrategia de comunicación?*

D → *¿Se informó al Consejo de Ética de Investigación de la colaboración con partidos políticos secesionistas?*

*146/ Carta del Sr. Ronald Deibert a Jordi Cañas, página 6. El Sr. Deibert alega que el trabajo de campo siguió un método de bola nieve basado en criterios de investigación específicos.*

De varios intercambios con la Oficina de la Integridad en la Investigación de la Universidad de Toronto entre junio y julio de 2022 puede deducirse que no se solicitaron ni concedieron permisos específicos en relación con la investigación en Cataluña, y que no se informó al Consejo de Ética de que los partidos políticos secesionistas estaban implicados en los análisis forenses y en la selección de los participantes en el informe. ¿Otorgó el Consejo de Ética de la Investigación Universitaria (REB) a Citizen Lab «carta blanca» para hacer todo lo que quisieran con lo relacionado con su proyecto Pegasus, que abarcaba una gran variedad de países y circunstancias políticas? Si este no es el caso, el REB debería seguir investigando el caso para asegurar que no hay más desviaciones de los protocolos de la Universidad de Toronto.

7

# El extraño origen y calendario de la investigación

El inicio de la investigación CatalanGate por parte de Citizen Lab también está rodeado de incoherencias y no está claramente justificado. El informe CatalanGate sostiene que la investigación en Cataluña se inició a raíz de una vulnerabilidad explotada por el grupo NSO para hackear teléfonos Android en todo el mundo con Pegasus a través de WhatsApp. WhatsApp paralizó esta vulnerabilidad y aprobó una lista de 1.400 usuarios que supuestamente eran objetivos del *spyware* Pegasus. Cabe suponer que, entre ellos, había varias figuras políticas en Cataluña. Citizen Lab ayudó a WhatsApp a notificar a las presuntas víctimas. Sin embargo, la denuncia formal de WhatsApp contra NSO (que citaba varias veces a Citizen Lab) mencionaba muchos países diferentes, nunca España.[147] Del mismo modo, ninguno de los informes anteriores elaborados por Citizen Lab en relación con la utilización de *spyware* NSO mencionaba presuntos ataques en Cataluña o en el resto de España.[148] Al mismo tiempo, el movimiento a favor de la independencia estaba sufriendo una fuerte disminución del apoyo público desde principios de 2019[149] que podría estar relacionado con el fracaso de la iniciativa del Tsunami Democràtic para de reunir el apoyo esperado una vez que la policía comenzara a neutralizar sus acciones.[150]

147/ *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

148/ *For instance, Bill Marczak & John Scott-Railton, The Citizen Lab, The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender 5 (24 de agosto de 2016),* https://tinyurl.com/y3uvmlev

*Bill Marczak et al., The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil, The Citizen Lab (1 de octubre de 2018),* https://tinyurl.com/y9yyhaz3

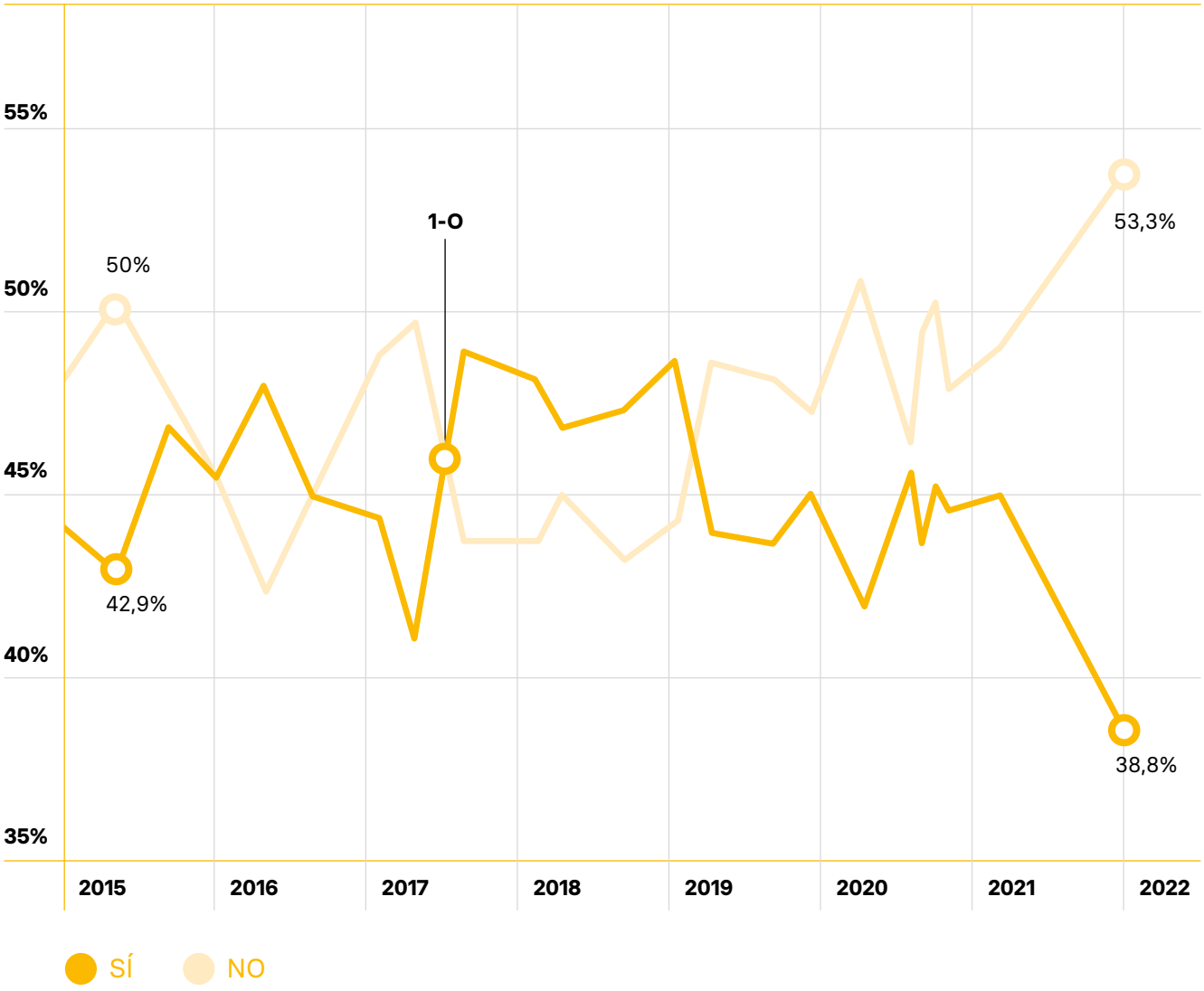
*John Scott-Railton et al., Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links, The Citizen Lab (11 de febrero de 2017),* https://tinyurl.com/ya3tgrhr.

149/ *El Mundo. El no a la independencia de Cataluña saca ocho puntos al sí y supera el 50%. 31 de julio 2020, https://www.elmundo.es/cataluna/2020/07/31/5f23f0ff21efa0eb258b4602.html*

150/ *El Periódico. Tsunami reconoce que "la gran acción no ha tenido éxito." 18 de julio de 2019, https://www.elperiodico.com/es/politica/20191218/tsunami-democratic-reconoce-poco-exito-accion-reivindicativa-clasico-7780485*

## TABLA 3

### APOYO A LA INDEPENDENCIA (ENERO 2015 – MARZO 2022)




*Fuente: El Confidencial basado en el Centre d'Estudis d'Opinió*

En una entrevista de televisión, Elies Campo se presenta como el coordinador del informe. Explica que en octubre de 2019 Citizen Lab empezó a ponerse en contacto con las presuntas víctimas de una violación de la seguridad de WhatsApp que tuvo lugar a principios de ese año. Al parecer, WhatsApp había encargado a Citizen Lab que se pusiera en contacto con las posibles víctimas de la sociedad civil. Según el libro del Sr. Torrent, el Sr. Scott-Railton confirmó el 9 de julio de 2020 lo siguiente:

«Como ustedes saben, colaboramos con WhatsApp. Nos transmiten información sobre los dispositivos que han intervenido y buscamos y encontramos a los propietarios de los móviles que han sido víctimas del espionaje... cuando ocurrió el incidente, intenté ponerme en contacto con el Sr. Torrent, pero no lo logré».[151]

Como se ha explicado anteriormente, el Sr. Campo afirma haber sido contactado por algunas de estas presuntas víctimas que habían sido advertidas de una posible infección y que sabían que había trabajado para Whatsapp algunos años antes. Le pidieron que comprobara si la violación de la seguridad había tenido lugar. El Sr. Campo afirma que se puso en contacto con antiguos compañeros de WhatsApp, quienes confirmaron que se había producido el espionaje. Tras ponerse en contacto con Citizen Lab y ofrecerle sus servicios, explicando que comenzó a coordinar la segunda fase de una investigación iniciada después de que los primeros casos se publicaran en julio de 2020,[152] sorprendentemente, el Sr. Campo afirma no recordar quién fue la primera víctima en Cataluña, aunque explica que descubrieron Pegasus en el ordenador del Sr. Joan Matamala a finales de julio o principios de agosto de 2020.

*151/ Torrent (2021) Pegasus, páginas 25-26*

*152/* *CCMA. TV3. 23 de abril de 2022. Preguntes Freqüents. El Catalangate amb John Scott-Railton i Elies Campo, Lang Lang i Noemí Casquet* https://www.ccma.cat/tv3/alacarta/preguntes-frequents/el-catalangate-amb-john-scott-railton-i-elies-campo-lang-lang-i-noemi-casquet/video/6155478/

El informe del CatalanGate dice que el Sr. Roger Torrent fue el primer líder independentista al que Citizen Lab y WhatsApp notificaron. Contrariamente a lo que el informe de CatalanGate afirma, el Sr. Torrent explica en su libro *Pegasus: L'Estat que ens espia*[153] y en una entrevista publicada en ARA,[154] que no recibió ninguna notificación de WhatsApp y que la primera notificación de su presunto ataque con Pegasus fue realizada por los periodistas Joaquín Gil (El País), Sam Jones (The Guardian) y Stephanie Kirchgaessner (The Guardian) el 8 de julio de 2020. Además, estos periodistas insistieron en que el Sr. Torrent se pusiera en contacto con Citizen Lab, y se refirieron específicamente a Ronald Deibert y John Scott-Railton.[155] La Sra. Kirchgaessner ha escrito docenas de artículos sobre Citizen Lab en The Guardian,[156] ha cubierto ampliamente casos espuestos por esta organización y ha entrevistado con frecuencia a los autores.[157]

*153/ Roger Torrent (2021). Pegasus: L'Estat que ens espia. Barcelona: Ara Llibres, página 14.*

*154/* *ARA. La novel·la d'espies de Roger Torrent, 5 de abril de 2021, https://www.ara.cat/politica/novel-d-espies-roger-torrent_1_3937649.amp.html*

*155/ Roger Torrent (2021). Pegasus: L'Estat que ens espia. Barcelona: Ara Llibres, página 14.*

*156/* *Stephanie Kirchgaessner, The Guardian. https://www.theguardian.com/profile/stephanie-kirchgaessner*

*157/* *Por ejemplo, The Guardian, UN rapporteur condemns UK hosting of Israeli spyware firm. 7 de febrero de 2020. https://www.theguardian.com/world/2020/feb/07/un-rapporteur-condemns-uk-hosting-of-israeli-spyware-firm*

*The Guardian. WhatsApp sues Israeli firm, accusing it of hacking activists' phones. 29 de octubre de 2019 https://www.theguardian.com/technology/2019/oct/29/whatsapp-sues-israeli-firm-accusing-it-of-hacking-activists-phones*

*The Guardian. Saudi Arabia accused of hacking London-based dissident. 28 de mayo de 2019 https://www.theguardian.com/world/2019/may/28/saudi-arabia-accused-of-hacking-london-based-dissident-ghanem-almasarir*

La Sra. Kirchgaessner es autora y coautora de muchos artículos sobre los ataques de Pegasus en Cataluña, incluyendo una exclusiva para The Guardian y El País que anunciaba que políticos secesionistas séniors en Cataluña habían sido supuestamente atacados con Pegasus el 13 de julio de 2020.[158]

La participación de periodistas en esta fase preliminar de un proyecto de investigación académica es muy poco habitual. ¿Cómo es que estos periodistas estaban teniendo la primera toma de contacto con el Sr. Torrent? ¿Pidieron el Sr. Scott-Railton u otra persona de Citizen Lab a los periodistas Stephanie Kirchgaessner, Sam Jones o Joaquín Gil que se pusieran en contacto con Roger Torrent y le advirtieran de que podría ser víctima del ciberespionaje? Si WhatsApp encargó a Citizen Lab que se pusiera en contacto con miembros de la sociedad civil a los que se atacaba con Pegasus, como explica el Sr. Elies Campo en una vista de televisión,[159] ¿por qué no lo hicieron directamente y por qué dependen de periodistas para un primer contacto? Incluso el Sr. Gil expresa el carácter poco habitual de este primer contacto en un mensaje dirigido al Sr. Joan Serra:

«Y la primera llamada que te hice fue extraña: ¡llamaba a un político para que pidiese a un canadiense que le dijese si había sido espiado!».[160]

158/ *The Guardian, Phone of top Catalan politician 'targeted by government-grade spyware', 13 de julio de 2020.* *https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware*

159/ *Preguntes Freqüents. El Catalangate amb John Scott-Railton i Elies Campo, Lang Lang i Noemí Casquet* *https://www.ccma.cat/tv3/alacarta/preguntes-frequents/el-catalangate-amb-john-scott-railton-i-elies-campo-lang-lang-i-noemi-casquet/video/6155478/*

160/ *Roger Torrent (2022). Pegasus, página 100.*

En un artículo de El País, el Sr. Gil explica que, según el abogado de la Sra. Anna Gabriel, Olivier Peter, no recibió ninguna notificación de WhatsApp informándole de que su móvil podría haber sido pirateado. Mientras tanto, en el mismo artículo, Jordi Domingo dice que el Sr. Scott-Railton lo llamó en octubre de 2019.[161] Si Citizen Lab tenía permiso para ponerse en contacto con personas incluidas en la lista de posibles víctimas en la violación de la seguridad de WhatsApp, ¿por qué implicaron a periodistas en este primer contacto con el Sr. Torrent? ¿Por qué, de los 1.400 usuarios de la lista de presuntas personas atacadas con programas espía de WhatsApp, decidieron centrarse en Cataluña en julio de 2020? A pesar de haber sido contactado en varias ocasiones, WhatsApp nunca ha respondido a ninguno de los mensajes relativos a la investigación de Citizen Lab en Cataluña.

Antes de la violación de la seguridad de WhatsApp, en 2018, Citizen Lab explicó que había identificado un total de 45 países en los que los operadores de Pegasus podrían estar llevando a cabo operaciones de vigilancia.[162] Mencionaron Baréin, Kazajistán, México, Marruecos, Arabia Saudí y los Emiratos Árabes Unidos, pero no España. Más de veinte países se vieron afectados por los ataques de programas espía contra la violación de la seguridad en WhatsApp. Por ejemplo, en septiembre de 2019, WhatsApp informó al Gobierno indio de que 121 personas se habían visto potencialmente comprometidas por el *spyware* Pegasus.[163] En la denuncia formal de WhatsApp Inc contra el grupo NSO[164] no se mencionaron España ni Cataluña, mientras que sí que se citaron varios regímenes autoritarios y países con déficits democráticos importantes.

Del mismo modo, el jefe de WhatsApp Will Cathcart, cuando fue entrevistado en The Washington Post sobre los ataques de Pegasus relacionados con la violación de la seguridad descubierta en 2019, no mencionó España ni Cataluña, sino que se refirió a países como Arabia Saudí, Francia, Sudáfrica, Irak, Pakistán, Egipto y Marruecos.[165] Además, en julio de 2021, el consorcio de periodismo Forbidden Stories, que también investiga Pega-

*Protesta en Gerona, 14 de octubre de 2019. Créditos usuario de Wikipedia Davidpar. CC BY-SA 4.0*

sus, con apoyo técnico de Amnistía Internacional, descubrió una fuga de más de 50.000 números de teléfono seleccionados para la vigilancia por los clientes del grupo NSO desde 2016.[166] En su web, hacen referencia a al menos 180 periodistas que son víctimas de programas espía, pero solo mencionan a un periodista español, Ignacio Cembrero, corresponsal del Magreb para El Confidencial.[167]

¿Cuál fue la verdadera motivación para elegir a España por delante de muchos otros países, con un historial mucho peor en materia de derechos humanos y Estado de Derecho, como los mencionados por WhasApp, las Forbidden Stories y los análisis anteriores de Citizen Lab? ¿Por qué le preocupaba a Citizen Lab un caso en el que varias de las personas cuyos teléfonos estaban supuestamente infectados eran objeto de una investigación flagrante debido a su participación en actos ilícitos?

161/ *El País. El móvil del presidente del Parlament fue objetivo de un programa espía que solo pueden comprar Gobiernos. 14 de julio de 2020. 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*

162/ *By Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert (2018). Hide and Seek:Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/*

163/ *Indian Express. In September, WhatsApp told govt 121 individuals affected by Pegasus spyware. 3 de noviembre de 2019, https://indianexpress.com/article/technology/whatsapp-israeli-spyware-snooping-pegasus-indian-government-6099262/*

164/ *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*

165/ *Chief of WhatsApp, which sued NSO over alleged hacking of its product, disputes firm's denials on scope of, involvement in spyware operations, 24 de julio de 2021, https://www.washingtonpost.com/investigations/2021/07/24/whatsapp-pegasus-spyware/*

166/ *Forbidden Stories. About The Pegasus Project. https://forbiddenstories.org/about-the-pegasus-project/*

167/ *Forbidden Stories. Journalists Under Surveillance. https://forbiddenstories.org/pegasus-journalists-under-surveillance/*

Por ejemplo, Roger Torrent y Anna Gabriel fueron investigados por cargos de desobediencia, siendo esta última una fugitiva de la justicia en el marco de una orden de búsqueda internacional.[168] Sergi Miquel fue investigado por su participación en Tsunami Democràtic[169], así como el Sr. Jordi Domingo debido a su participación en un grupo que coordinaba acciones ilegales para tomar el control de Cataluña y promover una criptomoneda catalana para eludir el control fiscal español[170].

Cuando se preguntó al Sr. Deibert sobre su elección de España de entre los más de 20 países afectados por los ataques de programas espía revelados por WhatsApp, no justificó claramente la elección, sino que se limitó a afirmar que «Citizen Lab es un laboratorio de investigación independiente con sede en la Universidad de Toronto y no sigue órdenes de investigación de empresas o gobiernos»[171].También alegó que estaban investigando países como Togo, Ruanda y otros en relación con el incumplimiento del compromiso de WhatsApp de 2019, que «en ningún caso levarían a cabo una investigación bajo encargo»[172] y que «ninguna otra institución o grupo participó en el análisis forense realizado para el informe»[173].

Sin embargo, en el caso de la investigación en Cataluña, parece evidente que Citizen Lab puede haber seguido instrucciones, así como haber recibido asistencia técnica en el análisis de los teléfonos y la identificación de las presuntas víctimas, de partidos secesionistas (ERC, JxCat y CUP), activistas políticos (como el coautor Sr. Campo y las organizaciones separatistas ANC y Òmnium) e incluso de organizaciones gubernamentales catalanas como la Agència de Ciberseguretat de Catalunya. Los testimonios de Roger Torrent, Oriol Tortuella y Van den Eynde[174] confirman que las declaraciones del Sr. Deibert no eran veraces. En una entrevista en La Vanguardia, el Sr. Tortuella explicó que esta agencia colaboró estrechamente con Citizen Lab en los exámenes forenses iniciales. Y lo que es más importante, también confirma lo que Roger Torrent había revelado en su libro, que los partidos secesionistas ERC, JxCat y CUP y las organizaciones políticas Òmnium y ANC colaboraban institucionalmente en la selección de los dispositivos que el Citizen Lab debía comprobar. El Sr. Torrent escribe que ni siquiera necesitaron científicos informáticos para afianzar los mensajes sospechosos y que «se han convertido en expertos rastreadores». Andreu Van Den Eynde explicó en la Comisión de Investigación PEGA que Citizen Lab, Amnesty Tech y su propio equipo de expertos participan en los análisis forenses[175].

La participación de organizaciones secesionistas catalanas en el trabajo de campo y la campaña de comunicación y el hecho de que solo se analizaran los teléfonos de políticos y activistas secesionistas demuestran que este estudio no fue guiado por consideraciones neutras de investigación. La decisión de conceder tanta fuerza al caso de Cataluña, la fe demostrada en la existencia de un espionaje masivo mucho más allá de las cinco presuntas víctimas teóricas de la lista de WhatsApp y el margen de maniobra concedido a los agentes secesionistas en la investigación parecen sugerir que o bien Citizen Lab se había encargado efectivamente de esta investigación o incluso que se trataba principalmente de una investigación dirigida por entidades ca-

talanas, en la que el papel de Citizen Lab era principalmente dar legitimidad a las acusaciones contra España. Como se verá en la siguiente sección, las numerosas contradicciones relativas a los testimonios de autores y participantes parecen corroborar que no se trataba en modo alguno de un proyecto normal de investigación universitaria, planificado y ejecutado de acuerdo con los principios académicos.

168/ *ABC. Anna Gabriel, la líder de la CUP que cumple dos años fugada de la justicia. 20 de febrero de 2022, https://www.abc.es/espana/catalunya/politica/abci-anna-gabriel-lider-cumple-anos-fugada-justicia-202002201731_noticia.html?ref=https%3A%2F%2Fwww.google.com%2F*

*Eldiario.es. Puigdemont, la principal carpeta del procés en los tribunales a la espera de la desjudicialización. 1 de octubre de 2022, https://www.eldiario.es/catalunya/puigdemont-principal-carpeta-proces-tribunales-espera-desjudicializacion_1_9581694.html*

169/ *El gobierno de Sánchez autorizó el espionaje a 18 dirigentes del Tsunami Democràtic, según 'El Confidencial'. 28 de abril de 2022, https://es.ara.cat/politica/gobierno-sanchez-autorizo-espionaje-18-dirigentes-tsunami-democratic-confidencial_1_4353964.html*

170/ *20 Minutos. La Guardia Civil sitúa a empresarios e informáticos en el 'CNI catalán' que se reunió con CDR para aupar la república, 22 de octubre de 2022, https://www.20minutos.es/noticia/5070783/0/la-guardia-civil-situa-a-empresarios-e-informaticos-en-el-cni-catalan-que-se-reunio-con-cdr-para-aupar-la-republica/*

*El País. Pegasus espió a uno de los promotores de la criptomoneda catalana. 2 de mayo de 2022, https://elpais.com/espana/2022-05-02/pegasus-espio-a-uno-de-los-promotores-de-la-criptomoneda-catalana.html*

171/ *Carta del Sr. Ronald Deibert a Jordi Cañas, página 5.*
172/ *Carta del Sr. Ronald Deibert a Jordi Cañas, página 6.*
173/ *Carta del Sr. Ronald Deibert a Jordi Cañas, página 3.*

174/ *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; Torrent (2021) Pegasus. página 142.*

175/ *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*

*Torrent (2021) Pegasus. pp. 142-143; Parlamento Europeo, Centro Multimedios, Comisión de Investigación para investigar el uso del programa espía de vigilancia Pegasus y otros programas equivalentes, 28 de noviembre de 2022, https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20221129-0900-COMMITTEE-PEGA*

# 8

# Otras contradicciones en las que incurrieron los autores del informe

Como se ha explicado anteriormente, en el ámbito de la criminalística digital es extremadamente importante que especialistas formados realicen los análisis, garanticen la custodia de las pruebas y la documentación de los procesos, con el fin de preservar la integridad de los datos, evitando la pérdida o alteración de información. Por desgracia, en el testimonio de autores y participantes en la investigación pueden detectarse algunas contradicciones pertinentes que sugieren una falta de adherencia a unos estándares académicos mínimos en la investigación del CatalanGate.

El Sr. Deibert afirma que «no participaron otras instituciones o grupos en el análisis forense realizado para el informe», más allá del examen de cuatro muestras por Amnesty Tech.[176] Sin embargo, esta afirmación no solo contradice los testimonios de los Sres. Torrent y Tortuella (véase el apartado anterior), sino también choca con lo descrito en el mismo informe «CatalanGate», que explica que la infección «Candiru» había sido identificada en el campus de la Universidad de Girona, en el dispositivo del Sr. Joan Matamala.

*176/ Carta del Sr. Deibert a Jordi Cañas, página 4.*

El estudio afirma que:

«Al llevar a cabo una investigación preliminar sobre los programas espía Candiru encontramos pruebas de una infección viva de Candiru en una red troncal institucional utilizada por un consorcio de universidades catalanas».[177]

«Los compañeros de Matamala le pidieron que se alejara del ordenador y fuese al pasillo. Una vez explicada la situación, dio su consentimiento a un análisis forense del producto. Hemos podido extraer con éxito los programas espía maliciosos y determinar que se había instalado de forma persistente en su dispositivo».[178]

*177/ Scott-Railton et al. CatalanGate página 16*
*178/ Scott-Railton et al. Catalangate, página 16*

El Sr. Elies Campo explica en una entrevista televisiva que descubrió un caso de infección por Pegasus durante un análisis de redes sociales entre finales de julio y principios de agosto de 2020.[179] Describe que estaba investigando el origen de esta infección, pero que tuvo dificultades para identificar en qué edificio y en qué oficina estaba el dispositivo infectado. Por último, comprobaron que el propietario del aparato era el Sr. Joan Matamala y el análisis de su teléfono confirmó que había sido infectado con Pegasus. Meses más tarde, de nuevo a través de un análisis vía la red social, lograron localizar una infección por Candiru y el Sr. Campo encontró la misma IP que había encontrado antes al descubrir la infección por Pegasus del Sr. Matamala. Se pusieron de nuevo en contacto con él y confirmaron que su ordenador estaba actualmente infectado con Candiru.[180]

El Sr. Matamala —supuestamente el "paciente cero" de Candiru— fue cofundador, junto con Jordi Baylina, de la Fundació Nord[181], que promueve la tecnología blockchain para el voto electrónico y la creación de la infraestructura en línea necesaria para una Cataluña independiente[182].

Se plantean varias cuestiones:

A → *¿Quién realizó ese examen físico en la Universitat de Girona?*

B → *¿Llevó a cabo algunos de los exámenes la Fundación Nord con sede en Girona?*

C → *¿Cuántos dispositivos se examinaron en Cataluña?*

179/ *«Anàlisi de xarxes»*

180/ *CCMA. TV3. Pregunts freqüentsEl Catalangate amb John Scott-Railton i Elies Campo, Lang Lang i Noemí Casquet* https://www.ccma.cat/tv3/alacarta/preguntes-frequents/el-catalangate-amb-john-scott-railton-i-elies-campo-lang-lang-i-noemi-casquet/video/6155478/

181/ *Fundació Nord,* https://www.fundacionord.cat/en

182/ *Vilaweb. Joan Matamala: "El problema que tenim és que som massa obedients", 1 de mayo de 2022.* https://www.vilaweb.cat/noticies/joan-matamala-problema-massa-obedients/

D

→ *¿Quién examinó dichos dispositivos?*

E

→ *¿Se trataba de meras pruebas forenses preliminares? En caso afirmativo, ¿cuándo, dónde y por quién se realizaron los análisis forenses confirmatorios?*

F

→ *¿Por qué se omitieron las infecciones de Candiru en Cataluña en el informe «Hooking Candiru» de[183] en julio de 2021, pero posteriormente se incluyeron en el informe CatalanGate?*

G

→ *¿Por qué observa que el Sr. Matamala era «paciente cero» de la infección de Candiru cuando no había sido mencionado en el informe anterior?[184]*

La participación de secesionistas catalanes expertos en IT en la evaluación de los dispositivos del señor Matamala en la Universitat de Girona, contradice la afirmación del señor Deibert de que no se involucró a ninguna otra institución o grupo en los análisis de grupo. Dado que los detalles facilitados en algunos aspectos del informe, la ausencia de referencias a las fechas en que se realizaron los análisis en todos los casos es también inusual. No hay información sobre cuando fueron descubiertos por Citizen Lab los intentos de infección de Candiru contra Pau Escrich, Xavier Vives y Elies Campo.[185]

El Sr. Deibert no respondió a las preguntas sobre el número de dispositivos investigados, alegando que, para proteger la privacidad de los sujetos de investigación, Citizen Lab no comenta sobre los casos que no se publican ni divulgan públicamente. Sin embargo, esta cuestión sigue siendo pertinente y la justificación es insatisfactoria. La pregunta no implica ninguna amenaza a la privacidad, sino que es la práctica estándar en la investigación y la divulgación de positivos. Para tener una mayor comprensión de la magnitud o la gravedad de la situación, es importante entender la proporción o los rangos de los positivos (p. ej., porcentaje de positivos/porcentaje de dispositivos testeados).

183/ *Bill Marczak, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ron Deibert (2021). Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus. Citizen Lab, 15 de julio de 2021, https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/*

184/ *John Scott-Railton, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, y Ron Deibert (2022). CatalanGate; Amplia operación Mercenary Spyware contra catalanes que utilizan Pegasus y Candiru. Citizen Lab, 18 de abril de 2022, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, Page 16*

185/ *"Anàlisi de xarxes"*

Por ejemplo, 65 positivos de 100 pruebas sería mucho más preocupante que 65 de 1.000. Una relación muy alta de positivos/dispositivos probados también puede ser un indicador de un problema instrumental con el software de detección de programas espía. La reticencia a responder a esto puede interpretarse como un intento de ocultar una posible limitación de la investigación no divulgada.

El Sr. Deibert dio la misma respuesta a la pregunta de si también se investigaron dispositivos de líderes o activistas no secesionistas: «Para proteger la privacidad de los sujetos de investigación, siguiendo el protocolo ético de investigación aplicable, el Citizen Lab no suele comentar casos que no se publican ni se divulgan públicamente». En este caso, la justificación aportada no es lógica y sugiere, una vez más, un intento anormal de evitar el control externo de decisiones de investigación potencialmente cuestionables. Revelar si objetivos no secesionistas han estado entre los estudiados no implica revelar sus nombres. Explicar la lógica del muestreo es habitual en la investigación científica.

Cabe señalar que, tras la publicación de la entrevista del Sr. Oriol Tortuella en La Vanguardia, en la que se refiere a la implicación de la Agència de Ciberseguretat de Catalunya en los análisis, el Sr. Deibert acusó al periódico de mentir y solicitó una retracción a través de Twitter. Sin embargo, más tarde cambió de opinión, suprimió su tweet acusatorio y reconoció parcialmente:

«En aras de la transparencia: acabo de borrar un tuit anterior relativo a la historia @LaVanguardia. De hecho, hemos mantenido algunos intercambios formales previos con la Agència de Ciberseguretat de Catalunya en el pasado».[186]

Esta reacción parece mostrar que, o bien el Sr. Deibert estaba nervioso sobre el conocimiento público de la participación de varios grupos en los análisis técnicos de los teléfonos que más tarde sirvieron para atribuir el victimismo y la culpa, o bien que el Sr. Deibert no sabía realmente cómo se llevó a cabo el trabajo de campo, lo que contradice su afirmación relativa a la supervisión y la independencia del Sr. Campo, así como a la dirección efectiva del trabajo de campo en Cataluña.[187]

*186/* *Ronald Deibert @RonDeibert. Twitter, 9 de mayo de 2022, https://twitter.com/RonDeibert/status/1523731577926479872?t=VguA5TGNQmy2M2uUfsj2MQ&s=19*

*187/* *Carta del Sr. Deibert a Jordi Cañas, página 3.*

El Sr. Campo también explica que la investigación siguió un proceso de muestreo algo inusual. En una entrevista, admite que preguntaba a las personas si querían que se comprobasen sus teléfonos para ver si habían sido atacados o infectados. A continuación, preguntaron a las presuntas víctimas:

## «si usted fuera el atacante y supiera todo lo que sabe y todas las personas con las que ha interactuado, enviado mensajes o llamado, ¿a quién atacaría?».[188]

Este enfoque no parece ajustarse plenamente a ningún criterio teórico específico de investigación, como suele esperarse en la investigación académica. El informe CatalanGate evita explicar o justificar los criterios seguidos en el muestreo de bola de nieve.

Una de las participantes, la Sra. Sonia Urpí, miembro del consejo de la ANC, proporcionó un vídeo testimonio sobre su caso[189] que también parece contradecir algunas de las explicaciones dadas por Citizen Lab. En el vídeo afirma que descubrió su infección telefónica en julio de 2020 justo después de su pareja, Jordi Baylina, empresario informático, presunta víctima e investigado por el Tribunal Supremo por su participación en el Tsunami Democràtic, descubrió durante un control de seguridad rutinario que su teléfono había sido pirateado. Le pidió que analizara su propio teléfono. Citizen Lab y el Sr. Torrent sugieren que los periodistas El País y The Guardian eran los que iniciaron la investigación en Cataluña a raíz de la lista facilitada por WhatsApp. ¿Por qué se excluyeron los casos de la Sra. Urpí y del Sr. Baylina? ¿Fue una coincidencia que un control rutinario detectara su infección?

188/ *CCMA. TV3. Preguntes frequents. El Catalangate amb John Scott-Railton i Elies Campo, Lang Lang i Noemí Casquet, 23 de abril de 2022, https://www.ccma.cat/tv3/alacarta/preguntes-frequents/el-catalangate-amb-john-scott-railton-i-elies-campo-lang-lang-i-noemi-casquet/video/6155478/*

189/ *Assemblea. Sonia Urpí #CatalanGate. Youtube. 26 de abril de 2022. https://www.youtube.com/watch?v=jH6Q1ZFLUm0*

El testimonio de la Sra. Urpí contradice el de su pareja, el Sr. Baylina, que, en una entrevista de televisión de 30 de abril de 2022, afirmó haber conocido la infección por Pegasus durante 5, 6 o 7 meses.[190] Esto significa que el Sr. Baylina tuvo conocimiento de la infección en 2021 y que ni la Sra. Urpí ni el Sr. Baylina dicen la verdad sobre cuando descubrieron sus supuestas infecciones. Baykiba afirma que el Sr. Elies Campo le contó sobre su trabajo en la investigación de Pegasus y que había sido espiado tras recibir algunos mensajes extraños. El Sr. Baylina dijo al Sr. Campo que también había recibido mensajes extraños en 2020. El Sr. Campo le pidió que le enviara «su teléfono o una copia» para poder analizarlo y, al parecer, descubrió que el teléfono del Sr. Baylina también estaba infectado. El Sr. Baylina también confirma que había visitado al Sr. Puigdemont en Bélgica «dos o tres veces» para debatir la estrategia de blockchain del movimiento independentista.

En el mismo programa de televisión, Gonzalo Boye, abogado de los Sres. Puigdemont y Torra y presuntamente víctima de espionaje, afirma que lo sabían «desde hacía algún tiempo», pero que «no disponían de pruebas para decirlo y demostrarlo. Ahora las tenemos»[191]. También dice que tenían la intuición de que estaban siendo espiados y que «hace más de dos años empezamos a intentar de obtener evidencia de ello y, finalmente, todas las pruebas han aparecido porque se ha realizado un análisis forense muy serio, muy riguroso y, sobre todo, independiente». Esta afirmación sugiere que, en 2020, cuando el caso de Pegasus en Cataluña fue publicado por importantes medios de comunicación internacionales y se presentó la demanda de los Sres. Torrent y Maragall, el movimiento separatista no parecía tener prueba alguna del espionaje.

*190/* *CCMA.cat. TV3. Preguntes frequents. Jordi Baylina: "He assumit que visc amb un mòbil espiat". 30 de abril de 2020, https://www.ccma.cat/tv3/alacarta/preguntes-frequents/jordi-baylina-he-assumit-que-visc-amb-un-mobil-espiat/video/6156617/ min 2.*

*191/* *CCMA.cat. TV3. Preguntes Freqüents. Gonzalo Boye: "Hem sigut espiats i hi ha proves". 30 de abril de 2022. https://www.ccma.cat/tv3/alacarta/preguntes-frequents/gonzalo-boye-hem-sigut-espiats-i-hi-ha-proves/video/6156598/*

Mientras tanto, la Sra. Diana Riba, presunta víctima y vicepresidenta de la Comisión de Investigación PEGA, alegó en una audiencia celebrada en París en el Consejo de Europa el 12 de diciembre de 2022, que Citizen Lab había detectado dos infecciones en su teléfono, la primera en junio de 2019, cuando supuestamente discutía con su partido y abogados sobre cómo defender al Sr. Oriol Junqueras.[192] Sin embargo, en el informe, la Sra. Riba solo parece ser víctima de una infección en torno al 28 de octubre de 2019.[193] Esta primera infección era conveniente para la estrategia independiente de censurar la nulidad de los juicios contra sus dirigentes, basada en el presunto seguimiento ilegal de abogados y de los debates jurídicos privados. Sin embargo, no se reflejó en el informe.

Aunque el Sr. Antoni Comín testificó como víctima en la Comisión PEGA el 6 de octubre de 2022,[194] el 22 de diciembre de 2022, Citizen Lab publicó una declaración en la que reconocía haber cometido un error identificando al Sr. Comín como víctima de Pegasus. Afirman que cometieron un error con sus sistemas de etiquetado y afirmaron erróneamente que las iniciales AC hacían referencia al Sr. Comín.[195] La explicación que figura en esa nota suscita nuevas dudas sobre el rigor en la codificación y el etiquetado de las pruebas. Ninguna víctima de la denuncia tiene AC como iniciales.

Esta afirmación también hace una alegación extraña: «Aunque no tenemos ninguna indicación forense de infección en los dispositivos de Comín que hemos comprobado, el dispositivo principal utilizado durante un período en el que otros fueron objeto de intentos de infección nunca ha estado disponible para su análisis debido a que el propietario no se acordaba de la contraseña». En su intento de sugerir la posibilidad de que el Sr. Comín siga siendo víctima, revelan otro hecho problemático. El Sr. Comín declaró en la comisión PEGA sabiendo que su

192/ *PACE public hearing: Pegasus and similar spyware and secret state surveillance. Youtube. 12 de diciembre de 2022. https://www.youtube.com/watch?v=zZft_l0cWJs*

193/ *Scott-Railton (2022). Catalangate, página 27.*

194/ *European Parliament. Multimedia Centre. Committee of Inquiry to investigate the use of the Pegasus and equivalent surveillance spyware. 6 de octubre de 2022, 10:09:21. https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20221006-0900-COMMITTEE-PEGA*

195/ *Ron Deibert (2022). CatalanGate Report Correcting a Case. 22 de diciembre de 2022, https://citizenlab.ca/2022/12/catalangate-report-correcting-a-case/*

teléfono principal nunca había sido analizado. Incluso explicó entonces por qué su espionaje había comenzado en enero de 2020 y lo vinculaba con un acto que organizó en Francia. Los miembros de la comisión y el público general deberían haber sido informados por el señor Comín de esta seria limitación al valorar su testimonio como «víctima».

En una entrevista en El País, se informa al Sr. Deibert de que los servicios secretos españoles solo han reconocido el seguimiento de 18 de los 65 casos mencionados en el informe. Reaccionó diciendo: «¿Cómo podemos verificarlo? ¿Qué han mostrado en la Comisión de Secretos Oficiales del Congreso? ¿Os lo creeríais?»[196]

Parece que se trata de un escepticismo sano, aunque algo incoherente. ¿Por qué espera el Sr. Deibert que la comunidad científica entienda sus acusaciones contra España, basadas en "evidencia circunstancial" (expresión literal del estudio de Citizen Lab) no revisada por pares y no replicada, al tiempo que cuestiona la respuesta del Gobierno español, por revelar solo información parcial (debido a la obligación impuesta por la Ley de Secretos Oficiales)? Normalmente, la carga de la prueba recae en el acusador y no en el acusado. En teoría, no corresponde al Gobierno español demostrar que no ha infringido la ley.

La sección del informe de Citizen Lab titulada «Atribución a un Gobierno» afirma:

→ *En este momento, Citizen Lab no está atribuyendo de manera concluyente estas operaciones de piratería informática a un gobierno concreto; sin embargo, una serie de pruebas circunstanciales apuntan a un fuerte nexo con una o más entidades del Gobierno español, entre ellas:*

- → *Los objetivos eran de interés evidente para el Gobierno español;*
- → *El calendario específico de los ataques coincide con eventos de especial interés para el Gobierno español;*
- → *El uso de contenidos de cebo en SMS sugiere el acceso a información personal de los objetivos, como los números de identificación españoles;*
- → *Al parecer, el CNI ha sido un cliente del grupo NSO y, al parecer, el Ministerio del Interior de España posee una capacidad similar, sin especificar cuál.*

196/ *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-usan-pegasus-porque-tienen-apetito-de-espiar.html

Estos argumentos carecen de fuerza probatoria. Algunos de los objetivos eran de interés evidente para el poder judicial y las fuerzas de seguridad españolas. Pero otros también eran objetivos potenciales para otros actores políticos en Cataluña. De hecho, los políticos nacionalistas catalanes habían sido acusados de espiar a diferentes políticos, activistas y periodistas de esta Comunidad Autónoma unos años antes,[197], y el Gobierno catalán había mostrado interés en adquirir tecnología de espionaje[198]. En cuanto al momento de los intentos de infección, el informe muestra que Citizen Lab no tenía capacidad para determinar de manera fiable cuándo o incluso si se produjeron infecciones. Además, el informe no justifica de manera convincente este argumento, sino que se limita a formular esta alegación sobre la base de unos pocos exámenes y no de un análisis sistemático. Las empresas de programas maliciosos y programas espía utilizan con frecuencia mensajes institucionales falsos, por lo que el argumento de que los intentos de infección deben atribuirse al Gobierno español o a los servicios secretos carece de credibilidad. Por último, una filtración de un antiguo empleado del NSO es la única indicación de que España está utilizando Pegasus. Ni el Gobierno ni la empresa de programas espía lo han admitido. Pero, aunque España tuviera Pegasus, Citizen Lab no ha aportado ninguna prueba técnica de que las fuerzas de seguridad españolas utilizaran este programa espía contra políticos y activistas separatistas catalanes. Las democracias suelen adquirir programas espía para luchar contra el terrorismo, el tráfico de drogas, la delincuencia organizada, etc.

*197/* *Crónica Global. CiU y ERC impiden que se forme una comisión para estudiar los posibles espionajes del Cesicat. 26 de junio de 2014, https://cronicaglobal.elespanol.com/politica/ciu-erc-impiden-comision-investigacion-espionajes-cesicat_9123_102.html*

*Crónica Global, Estas son las pruebas del espionaje de los Mossos, 11 de enero de 2019, https://cronicaglobal.elespanol.com/politica/estas-pruebas-espionaje-mossos_213201_102.html*

*198/* *El Confidencial. ¿A quién quiere espiar la Generalitat? Los correos de Mossos con los espías italianos. 20 de julio de 2015, https://www.elconfidencial.com/espana/cataluna/2015-07-20/a-quien-quiere-espiar-la-generalitat-los-correos-de-mossos-con-los-espias-italianos_935025/*

*El Confidencial. Puigdemont intentó comprar en Israel material de espionaje por 27 millones. 19 de marzo de 2018, https://www.elconfidencial.com/espana/cataluna/2018-03-19/puigdemont-israel-espionaje-material-compra_1536960/*

Además, también es bastante extraño que un profesor de ciencias políticas como el Sr. Deibert muestre una comprensión tan escasa y sesgada de la política catalana y española, siendo coautor de un estudio en la materia. Por ejemplo, en un documental sobre la CatalanGate titulado «El espía en tu bolsillo», publicado en octubre en TV3, afirmó que «... en Cataluña como ustedes tienen esta situación con la Constitución y el hecho de que incluso el mero acto de abogar por la independencia se considere ilegal...»[199] Esta afirmación es objetivamente falsa, ya que los partidos políticos y el activismo independentistas no solo son legales, sino que, de hecho, controlan el gobierno regional y la mayoría de las instituciones públicas en Cataluña.

Más recientemente, el Sr. Deibert publicó un artículo en la revista Foreign Affairs en el que afirma que «parte de los ataques tuvieron lugar en el marco de negociaciones delicadas entre los Gobiernos catalán y español sobre la suerte de los separatistas catalanes que estaban encarcelados o exiliados»[200]. Sin embargo, las negociaciones a las que aludió el Sr. Deibert probablemente han tenido lugar entre el Gobierno de Pedro Sánchez y el Sr. Pere Aragonès después de septiembre de 2021, fuera del período de las infecciones que Citizen Lab afirma haber detectado.[201].

*199/* *CCMA.cat. TV3. Pegasus, l'espia a la butxaca. 16 de octubre de 2022, https://www.ccma.cat/tv3/alacarta/30-minuts/pegasus-lespia-a-la-butxaca/video/6180772/*

*200/* *Ronald Deibert (2022). The Autocrat in Your iPhone. Foreign Affairs. 12 de diciembre de 2022. publicación de enero/febrero 2023. https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert*

*201/* *El País. Sánchez y Aragonès blindan un diálogo sin plazos pese a sus posiciones muy alejadas. 15 de septiembre de 2021 . https://elpais.com/espana/2021-09-15/sanchez-y-aragones-blindan-un-dialogo-sin-plazos-pese-a-sus-posiciones-muy-alejadas.html*

*En febrero de 2020 se celebró una reunión entre los Gobiernos español y catalán, este último encabezado por el Sr. Torra, pero en aquel momento el Gobierno español se negó a debatir la liberación de los dirigentes catalanes en prisión y en aquel momento no se habían iniciado negociaciones al respecto. Por otra parte, las fechas de los presuntos ataques en los teléfonos de los participantes en dicha reunión bilateral no coinciden con lo siguiente:*
*reuniónanterior. El País. Así fue la mesa de diálogo: Tres horas de terapia sobre el origen de la crisis catalana. 27 de febrero de 2020, https://elpais.com/politica/2020/02/27/actualidad/1582834113_996408.html*

9

# ¿Un trabajo de campo condicionado por intereses económicos? Facilitando «munición» para los juicios

La abundancia de pruebas que sugieren que la investigación de CatalanGate tiene poco que ver con una investigación científica adecuada, teóricamente impulsada y rigurosa, puede interpretarse como una indicación de que bajo el trabajo de Citizen Lab exista, en este caso, un conjunto diferente de posibles incentivos. Por ejemplo, el experto en seguridad digital, Nadim Kobeissi afirmó, el 18 de julio de 2022, que «Citizen Lab está abordando un problema sumamente valioso y urgente: mercenarios digitales que funcionan de forma ilegal a través de programas maliciosos sofisticados de uso militar. Pero mienten cuando sugieren que lo están haciendo científicamente. Es una práctica empresarial claramente motivada por la política»[202]. «Para ser claro, no hay nada malo en la aplicación de una práctica empresarial por motivos políticos. Puedes tener una agenda política, un conjunto de objetivos y hacer campaña para lograrlo descubriendo campañas de programas maliciosos. No hay nada que plantee problemas. El problema consiste en disimularlo como académico»[203].

El Sr. Deibert afirma que «a Citizen Lab nunca se le ha encargado encontrar pruebas para una demanda por parte de ninguna de las partes en un litigio, incluido Apple. En ningún caso realizaríamos una investigación encargada» El libro del Sr. Torrent contradice al Sr. Deibert y revela un enfoque muy problematico a la investigación del Citizen Lab."[204]

*202/* *Nadim Kobeissi. Wikipedia. https://en.wikipedia.org/wiki/Nadim_Kobeissi Nadim Kobeissi @kaepora, Twitter 18 de julio de 2022, https://twitter.com/kaepora/status/1549008483978285063?s=20&t=5eOMTc-7GNOLlTX1UdUb4Q*

*203/* *Nadim Kobeissi @kaepora, Twitter 18 de julio de 2022, https://twitter.com/kaepora/status/1549011017375666176?s=20&t=5eOMTc-7GNOLlTX1UdUb4Q*

*204/ Mr Ronald Deibert a Jordi Cañas, página 6.*

En el informe CatalanGate se afirma lo siguiente:

«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».[205]

Ciertamente, la investigación académica no debe guiarse por la estrategia jurídica de las grandes empresas tecnológicas ni por intereses políticos partidistas. El testimonio de los participantes en el trabajo de campo como Torrent y muchas de las declaraciones y acciones públicas de los miembros de Citizen Lab demuestran que aportar pruebas para litigios fue un principio clave de la investigación Pegasus en Cataluña. Los intereses de Citizen Lab y de los políticos y activistas separatistas catalanes parecen sinérgicos en este caso. Ambos intentaron maximizar el número de ataques de Pegasus. Citizen Lab quería ayudar a crear un caso para que Apple demandara a NSO, como había hecho en 2021 para WhatsApp.[206] Han tenido éxito, a partir del 23 de noviembre de 2022, Apple anunció que demandaba al grupo NSO y una recompensa de 10 millones USD, así como cualquier indemnización por daños y perjuicios derivada de la demanda, por investigadores y abogados de cibervigilancia, mencionando específicamente a Citizen Lab y Amnesty Tech:

*205/ Roger Torrent (2022). Pegasus, página 135.*

*206/* *The Guardian. WhatsApp sues Israeli firm, accusing it of hacking activists' phones, 29 de octubre de 2019, https://www.theguardian.com/technology/2019/oct/29/whatsapp-sues-israeli-firm-accusing-it-of-hacking-activists-phones*

«Apple elogia a grupos como el Citizen Lab y Amnesty Tech por su trabajo innovador para identificar los abusos de cibervigilancia y ayudar a proteger a las víctimas. Para seguir intensificando esfuerzos como estos, Apple aportará 10 millones USD, así como pagará cualquier daño derivado de la demanda, a organizaciones que lleven a cabo actividades de investigación y promoción de la cibervigilancia.

Apple también apoyará a los investigadores consumados de Citizen Lab con asistencia técnica, análisis de amenazas y asistencia de ingeniería pro bono para ayudar a su misión de investigación independiente y, en su caso, ofrecerá la misma asistencia a otras organizaciones que realicen un trabajo crítico en este espacio».[207]

207/ *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-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/

Además, Apple reveló en otro comunicado de prensa el 6 de julio de 2022 que los 10 millones de dólares que prometieron en noviembre de 2021 a Citizen Lab, Amnesty Tech y organizaciones similares serían asignados por el Fondo de Dignidad y Justicia de la Fundación Ford. Justamente, el Sr. Deibert es una de las 5 personas que decidirán cómo se gastarán estos fondos (junto con representantes de Amnesty Tech, Access Now, The Engine Room y Apple). Esto parece contradecir la declaración formal emitida por el Sr. Deibert en el Parlamento Europeo, en la que afirmaba que Citizen Lab nunca había recibido pagos o donaciones de Apple, WhatsApp o Facebook[209].

Esas personas conocían la demanda de Apple contra NSO en julio de 2020 y explicaron a los políticos catalanes que estaban colaborando con ella, sugiriendo que la investigación de Citizen Lab en Cataluña no se inspiraba realmente en ningún tipo de consideración académica, sino por la oportunidad de analizar muchos iPhones de políticos y activistas nacionalistas catalanes que deseaban ser presentados como víctimas de España.

Según el testimonio de los participantes antes mencionados, Citizen Lab ya buscaba pruebas para ayudar a Apple a presentar una demanda contra NSO en julio de 2020. Sin embargo, todo el caso de Apple contra NSO se articula en torno a la explotación de FORCEDENTRY de «cero clic» que se descubrió en marzo de 2021, y se supone que todos los ataques tuvieron lugar entre febrero y septiembre de 2021.[210] Ello significa que Citizen Lab pudo haber estado buscando pruebas de un presunto ataque que aún no se había producido y del que no disponía de ninguna prueba. No se trata de una conducta académica estándar: parece sugerir que se encargó a Citizen Lab que encontrara pruebas de un delito que todavía no se había producido (lo que también niegan), o que intentaban convencer a Apple de que iniciara una acción judicial, ya fuera motivada por un posible beneficio monetario, o bien para dañar al grupo NSO, una empresa contra la que habían luchado durante algunos años.

Si el objetivo perseguido por Citizen Lab era proporcionar «munición» a los litigios judiciales, la investigación podría debilitarse desde un punto de vista técnico. Por ejemplo, esto podría provocar un sesgo en el diseño del trabajo de campo y en la forma en que se redactó el informe. El fuerte sesgo de selección

*209/ Carta Mr Ronald Deibert a Jordi Cañas, página 6.*

*210/* *Apple. Apple v NSO Complaint, 23 de noviembre 2021, https://www.apple.com/newsroom/pdfs/Apple_v_NSO_Complaint_112321.pdf, páginas 2 y 13*

*Marczak et al. (2021). FORCEDENTRY : NSO Group iMessage Zero-Click Exploit Captured in the Wild, 13 de septiembre de 2021, Citizen Lab. https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/*

—solo los móviles de activistas y políticos nacionalistas fueron analizados— y la lectura muy unilateral sobre el conflicto de Cataluña, son prueba de estos potenciales problemas inducidos. Incluso el llamativo título del informe, un término introducido por el político separatista Maragall[211] y utilizado en una campaña de propaganda orquestada[212], sugiere una falta de rigor y el intento de crear un estado de opinión específico, una especie de pánico moral e indignación.

Si los móviles de políticos y activistas catalanes separatistas también formaban parte de una investigación en nombre de Apple, Citizen Lab debería reconocerlo en el informe CatalanGate. También debe documentar información relacionada, como el momento en que Apple solicita apoyo técnico en relación con las infecciones de programas espía iOS. ¿Cuándo descubrió Citizen Lab la intención de Apple de demandar a NSO? ¿Constituiría una infracción del Código Ético de la Universidad de Toronto la realización de investigaciones impulsadas por recompensas no divulgadas de empresas privadas o fundaciones vinculadas a ellas? ¿Sería una violación del código ético de la Universidad de Toronto adaptar los procesos de muestreo y el diseño de la investigación a los intereses de empresas privadas o partidos políticos? ¿Y qué ocurre con la filtración de información confidencial a la prensa?

La búsqueda por parte de Citizen Lab de infecciones en Apple parece verse confirmada por el hecho de que, después de los primeros casos en la lista de WhatsApp, y a pesar de la muy elevada cuota de mercado de Android en España, Citizen Lab centró sus análisis casi exclusivamente en políticos con iPhones. El Sr. Elies Campo justificó esta decisión ante políticos de ERC alegando que el análisis de los dispositivos Apple era más fiable que el de los dispositivos Android.[213]

Mientras tanto, políticos y activistas nacionalistas catalanes buscaron pruebas para presentarse como «víctimas» en un momento en el que muchos de ellos estaban siendo investigados por tribunales y fuerzas de seguridad españoles por colaboración con servicios secretos rusos en una operación de desestabilización de España, por casos de corrupción, de malversación de fondos públicos y de coordinación de una insurrección civil que permitiría a las fuerzas secesionistas luchar por el control del territorio al Gobierno español. Un número muy elevado de positivos ayudó a los partidos secesionistas a presentar previamente las investigaciones sobre estos crímenes como una represión estatal injustificada.

*211/ Torrent (2021). Pegasus, página 80*

*212/* *El Triángulo. «Catalangate», un Montaje propagandístico preparado el mínimo Detalle desde hace meses. 22 de abril de 2022, https://www.eltriangle.eu/es/2022/04/22/catalangate-un-montaje-propagandistico-preparado-hasta-el-minimo-detalle-desde-hace-meses/*

*213/ Torrent (2022). Pegasus, página 135.*

Aparentemente, el objetivo último de la investigación no era contribuir a ningún tipo de debate teórico ni a un análisis comparativo serio, sino aportar pruebas para los juicios y para una campaña de comunicación en los medios. Por ejemplo, el 17 de julio, antes de la confirmación forense de cualquier infección, el Sr. Scott-Railton puso en contacto al responsable de prensa del Sr. Torrent, Joan Serra, con el Sr. Luis Fernando García, abogado y director de la organización mexicana R3D. Quien invitó a los políticos de ERC a ponerse en contacto con Citizen Lab para obtener ayuda para detectar ataques y denunciar el caso en los medios de comunicación y en los tribunales.[214]

El Sr. Torrent también explica que, «a raíz de la investigación del caso Mansoor, la reputación de Citizen Lab se consolidó hasta el punto de que WhatsApp los contrató para la investigación del incidente de WhatsApp»[215]. Asimismo, «el objetivo de todas las investigaciones posteriores es relacionar la crisis de seguridad del incidente de WhatsApp con Pegasus»[216]. Estas declaraciones no solo contradicen la deontología de la investigación académica la investigación trata de establecer deliberadamente una hipótesis concreta, sino también las declaraciones formales del Sr. Deibert en respuesta a la mencionada carta de eurodiputados de Renew Europe. La extraordinaria atención que Citizen Lab dedica a Pegasus y a NSO en relación con otros programas espía resuena con la afirmación del Sr. Torrent. En los últimos años, Citizen Lab ha dirigido principalmente su trabajo y sus críticas contra los gobiernos y NSO, y muy rara vez se ha centrado en investigar las amenazas a la privacidad y la falta de rendición de cuentas de las grandes tecnológicas. Esto contrasta con el trabajo de esta institución hace años. El papel que Citizen Lab parece adoptar está más estrechamente relacionado con el de un agente industrial, una especie de «investigador contratado», que con el de un organismo independiente de investigación universitaria.

El 14 de julio, los Sres. Torrent, Sagrera y Andreu Van den Eynde, abogados de líderes secesionistas de ERC, que también fueron incluidos en el informe como «víctimas», empezaron a trabajar en una narrativa para una demanda, según el libro del Sr. Torrent:

*214/ Torrent (2022). Pegasus, página 111.*
*215/ Torrent (2022). Pegasus, página 23.*
*216/ Torrent (2022). Pegasus, página 26.*

«Ayudamos a Andreu a definir la historia: en primer lugar, tenemos el ataque al móvil acreditado por Citizen Lab; en segundo lugar, Pegasus, el software que solo se vende oficialmente a los servicios de inteligencia gubernamentales. Andreu afirma que, con el informe Citizen Lab, tenemos suficiente para apoyar la denuncia, pero que también nos gustaría contar con la confirmación de WhatsApp».[217]

«Bien, ahora solo tenemos que definir a quién nos dirigimos con la denuncia».[218]

El 16 de julio de 2020, antes de recibir confirmación de cualquier infeción, el Sr. Roger Torrent anunció en una entrevista por radio en Cadena SER que él y el Sr. Ernest Maragall presentaban una denuncia contra el antiguo director de los servicios secretos españoles, D. Félix Sanz Roldán, por espionaje con Pegasus.[219] Esta denuncia se basaba en una declaración de Citizen Lab que acreditaba que sus nombres figuraban en una lista de posibles víctimas del *spyware* Pegasus. El 18 de julio de 2020, según el libro del Sr. Torrent, Van den Eynde explicó que, tras ponerse en contacto con el equipo jurídico de WhatsApp, consideraba crucial obtener datos de WhatsApp para fundamentar su denuncia.[220]

*217/ Torrent (2022). Pegasus, página 71.*
*218/ Torrent (2022). Pegasus, página 72*

*219/* *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-querellaran-contra-exdirector-cni-felix-sanz-roldan-hackeo-telefonos-20200716100349.html*

*220/ Torrent (2022). Pegasus, página 135.*

¿A alguien de Citizen Lab le pareció sorprendente que los miembros de ERC con los que se habían puesto en contacto hubieran presentado una denuncia antes de obtener confirmación forense de cualquier infección en Cataluña? Por el contrario, Citizen Lab parecía estar a favor de la litigación: el 18 de julio de 2020, el Sr. Scott-Railton declaró:

> «Tu tema es la oportunidad de abrir un caso en la Unión Europea. Creo que hay suficientes elementos para que tu cuestión se convierta en una cuestión europea».[221]

Dado que aún no se había confirmado ninguna infección, ¿por qué el Sr. Scott-Railton estaba tan interesado en ayudar a los secesionistas catalanes a construir una causa judicial a escala europea? Esto demuestra que un interés fundamental para Citizen Lab era aumentar el perfil de su «lucha» contra el grupo NSO y generar indignación entre la opinión pública europea.

Dado que no se confirmaron nuevas infecciones, el escándalo Pegasus pareció disiparse gradualmente en otoño de 2020, tras una campaña de comunicación política internacional muy intensa por parte de políticos secesionistas y varias organizaciones y periodistas afines (véase la sección siguiente). Esto también podría formar parte de una estrategia centrada en la preparación del caso Apple, que se llevó a cabo en 2021. El retraso intencionado de la publicación de un informe que contenga datos pertinentes sobre presuntos delitos para satisfacer los intereses de partidos políticos o de empresas privadas podría considerarse una violación del código ético de la investigación académica, a menos que esté justificado. Como tal, es probable que, a pesar de toda la campaña de comunicación de 2020, Citizen Lab no tuviera pruebas sólidas de infecciones en Cataluña en ese momento.

Tras la publicación del informe CatalanGate, tanto los activistas nacionalistas como Citizen Lab comenzaron a trabajar en litigios. Por ejemplo, el 3 de mayo de 2022, el Sr. Gonzalo Boye presentó una nueva denuncia contra NSO,[222] en la que presenta a todos los coautores del informe CatalanGate para que expongan su testimonio de expertos, excepto el Sr. Campo, al que sorprendentemente ni siquiera menciona. Solicita al Sr. Marczak como testigo, y cita 14 veces a Citizen Lab y sus informes.[223] Ese mismo día, Joaquim Torra y Josep Costa anunciaron que presentaban otra denuncia contra el presidente del Gobierno español Pedro Sánchez, basándose en las conclusiones presentadas en el informe CatalanGate.[224] Es notable que, basándose en lo que el Citizen Lab admite como «pruebas circunstanciales», se hayan presentado muchas denuncias en los tribunales,

en España y en otros países. A 8 de mayo de 2022, los miembros de ERC, JxCat, ANC, Òmnium y CUP ya habían presentado demandas en Bélgica (Bruselas y Waterloo), Alemania (Berlín y Kehl), Luxemburgo, Suiza (Ginebra y Zúrich), Francia y España (Barcelona y Madrid) basándose en las conclusiones de la investigación CatalanGate.[225] La denuncia original de los Sres. Torrent y Maragall fue archivada el 30 de mayo de 2022, a raíz de la negativa de ambos políticos de proporcionar los dispositivos que afirmaban haber sido infectados para un examen forense. La excusa que dieron estos políticos era que ya no los tenían.[226] Esta justificación no es convincente, ya que sus teléfonos eran la principal prueba de incriminación en sus demandas.

*221/ Torrent (2022). Pegasus, página 114.*

*222/* *El Periódico. El abogado de Puigdemont se querella por al menos 19 ataques que ha sufrido con Pegasus, 3 de mayo de 2022, https://www.elperiodico.com/es/politica/20220503/abogado-puigdemont-querella-nso-espionaje-pegasus-13602811*

*223/* *Reclamación formal presentada por el Sr. Gonzalo Boye en Juzgado de Madrid de 3 de mayo de 2022, https://files.mediaset.es/file/10002/2022/05/03/Querella_Pegasus_-Gonzalo_BOYE-_-1-_-2_5367.pdf*

*224/* *El País. Quim Torra y el exvicepresidente del Parlament denunciarán a Pedro Sánchez por el espionaje de 3 de mayo de 2022, https://elpais.com/espana/catalunya/2022-05-03/quim-torra-y-el-exvicepresidente-del-parlament-denunciaran-a-pedro-sanchez-por-el-espionaje.html*

*225/* *El Independiente. El mapa de las querellas independientes 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/*

*226/* *RTVE. El juez archiva la causa por el espionaje a los teléfonos móviles de Torrent y Maragall. 30 de mayo de 2022, https://www.rtve.es/noticias/20220530/juez-archiva-causa-espionaje-moviles-torrent-maragall/2355780.shtml*

# 10

# ¿Una campaña de propaganda política?

La instrumentalización de los medios de comunicación para crear una sensación de urgencia ofreció a los políticos secesionistas catalanes la oportunidad de generar y representar una crisis política, como tienden a hacer los movimientos populistas en circunstancias similares (Moffitt 2015; Olivas Osuna, Rama 2021; Roberts 2022).[227] Esto es lo que intentaron en julio de 2020. Como refleja Roger Torrent en su libro, los medios de comunicación fueron clave para mantener viva la historia del espionaje a pesar de la falta de nuevas pruebas. Según su testimonio, The Guardian y El País fueron los medios de comunicación más importantes para legitimar sus reivindicaciones de victimismo. Menciona 27 veces en su libro al periodista de El País Joaquín Gil. El Sr. Gil fue la persona que, el 6 de julio de 2020, se puso en contacto por primera vez con el Sr. Torrent; el 8 de julio de 2020 junto con la Sra. Stephanie Kirchgaessner y el Sr. Sam Jones de The Guardian, advirtió a Torrent de que, en teoría, era objeto de un ataque de Pegasus. Además, estos periodistas insistieron en que el Sr. Torrent debería ponerse en contacto con Citizen Lab, y le remitieron al Sr. Ronald Deibert y al Sr. Scott-Railton.[228] el Sr. Torrent muestra un gran agradecimiento al Sr. Gil, que está decidido a luchar por el caso.[229] Antes de disponer de los resultados de cualquier análisis forense, el Sr. Gil ya había manifestado que creía que el caso iba a afectar a muchas más personas.

*227/* *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; 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; Roberts, K. M. (2022). Performing Crisis? Trump, Populism and the GOP in the Age of COVID-19. Government and Opposition, 1-19.*

*228/* *Torrent (2021), Pegasus, páginas 7-24.*

*229/* *Torrent (2021), Pegasus, página 61.*

Asimismo, cabe señalar que la reacción de las presuntas víctimas de los ataques parece ser de alegría, más que de preocupación, a la hora de encontrar indicios de que sus teléfonos podrían haber sido atacados. Por ejemplo, el Sr. Torrent, 11 de julio de 2020:

«09:30 h. Ya lo tenemos. Un mensaje de WhatsApp de Oriol (Sagrera) me informa de que esta noche recibimos el memorándum de Citizen Lab. Trabajan con rapidez. A pesar de la hermeticidad del mensaje, puedo imaginarme a Sagrera satisfecho y eufórico, como un buen alumno el día en el que recibe el boletín de notas. Todos tememos que, sin las pruebas sólidas que proporciona un memorándum, nadie se atreva a publicar la historia. Ahora los tenemos, y este documento empieza a disipar nuestros temores».[231]

«... el informe de Citizen Lab es la verificación oficial de que tenemos que hacer efectiva la reclamación...».[232]

«Hemos remitido el documento a Joaquín Gil y Sam Jones. Lo deseaban con aún más ansiedad que nosotros. Ahora disponen de un informe sólido para apoyar su investigación».[233]

Oriol Sagrera, jefe de gabinete de Roger Torrent y otra presunta víctima del espionaje, y el Sr. Scott-Railton comenzaron a supervisar el teléfono del Sr. Torrent un día antes. El memorándum recibido se limitó a afirmar que el teléfono del Sr. Torrent figuraba en la lista que WhatsApp había compartido con Citizen Lab. Aún no disponían de ninguna confirmación forense de infección, pero ya habían decidido presentar una reclamación ante los tribunales. Así, se representó a si mismo ante la prensa como una «víctima» al mismo tiempo que estaba siendo invesigado judicialmente como un potencial culpable. Como demuestra el Sr. Torrent en su libro, ese mismo día recibió un mensaje WhatsApp con un enlace a un artículo de La Vanguardia: «La Fiscalía está en posesión de los datos de la del Tribunal Constitucional contra Torrent» y lee un informe relativo a la investigación sobre cargos de desobediencia.[234]

Al día siguiente, el 12 de julio de 2020, los Sres. Gil y Jones consultaron al Sr. Torrent a través de Zoom para preparar sus próximos artículos sobre el presunto espionaje de Pegasus. Aún no se había recibido ninguna confirmación forense, ya que el seguimiento de la VPN no había concluido.[235]

El lunes 13 de julio, el Sr. Torrent solicitó, durante una reunión con el comité ejecutivo de ERC, que se activasen todos los protocolos de comunicación, ya que la noticia de que había sido infectado por Pegasus se iba a publicar ese miércoles; también debatieron cómo utilizarían la cuestión en sus relaciones con el Gobierno español. El Sr. Torrent debatió con sus colaboradores cercanos, Oriol Sagrera y Joan Serra, sobre cómo se producirían las primeras reacciones al anuncio en el boletín informativo del Telenotícies de TV3, y en una entrevista para RAC1 con Jordi Basté.[236]

El 13 de julio, el Sr. Gil comunicó al responsable de prensa del Sr. Torrent, Joan Serra, que le preocupaba que las noticias fueran públicas antes de publicarlas en El País, y que «el problema» es que, en este periódico, exigen un nivel mínimo de evidencias para verificar cada apartado, mientras que otros periódicos no necesitan documentación para publicar un informe. Sin embargo, justo después de medianoche, el Sr. Torrent celebra que tanto The Guardian como El País publicasen la exclusiva. Incluso el Sr. Torrent se sorprendió de que decidiera publicarlo pronto: «¡Están fuera! Hostia, temían que alguien fastidiara la exclusiva y lo han publicado»[237] Los dos artículos se basaron simplemente en el certificado enviado por Citizen Lab en el que se afirmaba que el teléfono del Sr. Torrent figuraba en una lista que WhatsApp les había dado.

*231/ Torrent (2021), Pegasus, página 40.*
*232/ Torrent (2021), Pegasus, página 41.*
*233/ Torrent (2021), Pegasus páginas 41-45.*

*234/* *La Vanguardia. La Fiscalía tiene ya encima de la mesa los datos del TC contra Torrent. 11 de julio de 2020, https://www.lavanguardia.com/politica/20200711/482217012988/fiscalia-tiene-mesa-datos-tribunal-constitucional-contra-torrent.html; Roger Torrent (2021), página 42.*

*235/ Torrent (2021), Pegasus, páginas 49-50.*
*236/ Torrent (2021), Pegasus, páginas 59-60.*
*237/ Torrent (2021), Pegasus, página 62.*

En el artículo de The Guardian, el Sr. Scott-Railton dice lo siguiente:

«Dada la naturaleza de este ataque y la limitada información recopilada por WhatsApp sobre sus usuarios, podemos confirmar que el teléfono fue objeto del *spyware*. Sin embargo, sería necesaria una investigación adicional para confirmar que el teléfono fue pirateado. En este momento, no tenemos motivos para creer que no lo haya sido».[238]

Esta última frase muestra una comprensión muy poco ortodoxa del análisis forense digital. No se debería considerar que los teléfonos estén infectados hasta que los análisis lo confirmen, y no al contrario. Es importante recordar que en ese momento todavía no había concluido ningún análisis forense.

El artículo de El País llega a afirmar que «los investigadores establecen un vínculo entre la sospechosa desaparición de los mensajes de WhatsApp en el móvil de Torrent en 2019 y una señal de manipulación e infección por terceros... Torrent participó, en mayo de 2019, cuando fue objetivo de Pegasus, en una reunión en Estrasburgo con la comisaria de Derechos Humanos del Consejo de Europa Duna Mijatovic». El País toma la memoria del Sr. Torrent desde 2019 como prueba de infección: «Estaba atento a cosas extrañas. Los mensajes de WhatsApp y los historiales de chat se borraron. Las personas que me rodean no tuvieron los mismos problemas».[239] Las fechas de infección del Sr. Torrent nunca fueron certificadas por ningún análisis forense.

*238/* *The Guardian. Phone of top Catalan politician «targeted by government-grade spyware». 13 de julio de 2020* https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware

*239/* *El País. 14 de julio de 2020. El móvil del presidente del Parlament fue objetivo de un programa 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

El artículo de The Guardian alegaba que la Sra. Anna Gabriel y el Sr. Jordi Domingo también habían sido espiados. ¿Por qué aparece el nombre del Sr. Torrent, junto con otros cuatro políticos y activistas separatistas catalanes, en una lista de teléfonos en torno a octubre de 2019, fue una gran página de portada exclusiva en The Guardian en julio de 2020? Dado que sabía que los teléfonos de algunos políticos y activistas catalanes separatistas figuraban en una lista de presuntos objetivos de Pegasus, ¿por qué ERC decide poner en marcha una campaña de comunicación a gran escala en julio de 2020, sin esperar a la confirmación forense de ninguna infección? La Sra. Anaïs Franquesa, abogada y colaboradora de la organización nacionalista catalana Òmnium, participó en un debate público en el que los Sres. Torrent y Maragall tuvieron conocimiento de sus infecciones al mismo tiempo que los demás políticos, pero decidieron lanzar la campaña en ese momento concreto debido a objetivos políticos legítimos.[240]

Le Monde y Vice se hicieron eco de las noticias sobre el espionaje del Sr. Torrent el 14 de julio de 2020 sin más confirmación de los hechos.[241] Ese mismo día, 8 partidos políticos, incluidos nacionalistas catalanes, vascos, gallegos y Podemos, solicitaron la creación de una comisión parlamentaria para investigar el espionaje de políticos catalanes por lo que denominan «las cloacas del estado».[242]

*240/* *Youtube. Canòdrom Ateneu d'innovació Digital I Democràtic. A l'ombra de Pegasus | Drets civils en la era de la vigilancia. 3 de noviembre de 2022. Min. 49: 35, https://www.youtube.com/ver? APP = ordenador de mesa («desktop») v = OcFBZBIWttY (característica OcFBZBIWttY) = emb_imp_ woyt. «Y me excusa, no es de tres meses, en realidad es mucho más, porque lo sabían (...). El momento de el espionaje de Ernest Maragall y Roger Torrent por parte de Pegasus [...] es el mismo que el resto (políticos y activistas). Evidentemente, y podemos decir, ¿por qué en este momento? Bien, sí, pero es la ciudadanía la que decide... la ciudadanía, y no me preocupa, con objetivos políticos, obviamente».*

*241/* *Le Monde. Des militantes catalanes visés par un logiciel espion ultraperfectionné, 14 de julio de 2020, https://www.lemonde.fr/pixels/article/2020/07/14/des-militants-catalans-vises-par-un-logiciel-espion-ultraperfectionne_6046138_4408996.html*

*Vicepresidente Fuente: España es cliente del grupo NSO, 14 de julio de 2020, https://www.vice.com/en/article/pkyzxz/spain-nso-group-pegasus-catalonia*

*242/* *El País. Podemos se suma a ERC y siete partidos para pedir una comisión sobre «las cloacas del Estado» tras el espionaje a Torrent, 14 de julio de 2020, https://elpais.com/espana/2020-07-14/podemos-se-suma-a-la-peticion-de-erc-y-siete-partidos-para-crear-una-comision-sobre-las-cloacas-del-estado.html?outputType=amp*

El 15 de julio, el Sr. Torrent fue entrevistado por el periodista Jordi Basté en el principal programa de radio de Cataluña en RAC1. Al parecer, en medio de la entrevista[243], el Sr. Basté le presentó al Sr. Elies Campo. El 16 de julio, Torrent recibe la confirmación de Citizen Lab de que su teléfono no estaba infectado. El Sr. Torrent afirma: «Tengo un teléfono móvil limpio. Es tranquilizador y decepcionante al mismo tiempo».[244] La campaña de comunicación rápida y de alcance lanzada por el movimiento separatista se estaba propagando sin ninguna base forense digital.

Sin embargo, ese mismo día, el Sr. Torrent y el Sr. Maragall enviaron cartas a la Sra. Dunja Mijatovic, Comisaria de Derechos Humanos del Consejo de Europa, a la Sra. 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[245]. En ese momento, estaban apoyando acusaciones contra España basándose únicamente en la confirmación de WhatsApp de que estos políticos estaban en una lista de 1.400 personas cuyos teléfonos habían sido atacados presuntamente por programas espía durante la violación de seguridad que se descubrió en la primavera de 2019, notificada a las posibles víctimas en otoño de 2019.[246] Se observa que las consideraciones políticas y no puramente investigativas comenzaron a dictar el camino de esta investigación, así como la comunicación pública de los resultados preliminares. Al parecer, el 21 de octubre de 2020, Amnistía Internacional envió una carta al Gobierno español solicitando una investigación sobre el espionaje de Pegasus contra políticos catalanes[247].

El 27 de julio, según el libro del Sr. Roger Torrent, Citizen Lab confirmó a ERC que ninguno de los teléfonos que habían enviado para su análisis estaba infectado, aunque afirmaba que algunos de los teléfonos tenían mensajes SMS que creían que eran ataques de Pegasus.[248] El 28 de julio, WhatsApp también expresó en The Guardian que no tenían pruebas de que se hubiera pirateado con éxito a los políticos y activistas catalanes

*243/* *Torrent (2021) Pegasus, página 76. Se presume que este fue el primer encuentro entre los Sres. Torrent y Campo. Basté había entrevistado previamente al Sr. Campo en 2019 en un programa de televisión en el que se presenta como empleado de Telegram. CCMA.cat. TV3. No pot ser! Elies Campo: el català que va fugir de WhatsApp quan va conèixer Facebook per dins. 14 de abril de 2019, https://www.ccma.cat/tv3/alacarta/no-pot-ser/elies-campo-el-catala-que-va-fugir-de-whatsapp-quan-va-coneixer-facebook-per-dins/*

*244/* *Torrent (2021) Pegasus, página 104.*

*245/* *Roger Torrent (2021). Pegasus, páginas 152-153.*

*246/* *Scott-Railton et al. (2022). CatalanGate, página 1.*

*247/* *Torrent (2021). Pegasus, página 70.*

*248/* *Torrent (2021) Pegasus, página 151.*

*249/* *El País. 14 de julio de 2020. 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*

separatistas de la lista.[249] Además, según el apéndice del informe CatalanGate, ninguno de los casos de la lista supuestamente notificados por WhatsApp confirmaba de forma forense la infección de Pegasus: se trata de Anna Gabriel, Ernest Maragall, Jordi Domingo, Roger Torrent y Sergi Miquel.

Es difícil entender cómo, dada la ausencia de infecciones confirmadas en Cataluña a finales de julio de 2020, una institución de investigación de una universidad como Citizen Lab decidió seguir dedicando recursos a España, cuando hubo muchos casos sospechosos de infecciones por Pegasus en dictaduras y en países con malos antecedentes en materia de derechos humanos. El 1 de noviembre de 2020, la prensa española comienza a publicar información procedente de una investigación policial —basada fundamentalmente en audios de conversaciones privadas— que demuestra los vínculos entre el movimiento secesionista y Rusia, y apunta a una red que organiza y financia ilegalmente a Tsunami Democràtic, en la que participaron varias personas implicadas en la investigación CatalanGate.[250] Testimonios indican que las organizaciones catalanas secesionistas fueron las más interesadas en encontrar infecciones por Pegasus. El hecho de que, al parecer, el Sr. Campo siguiera trabajando en la cuestión, sin estar afiliado a Citizen Lab, y de que el Sr. Torrent y otros líderes nacionalistas estuvieran convencidos de que encontrarían infecciones indican que el movimiento secesionista promovía activamente la investigación y que su trabajo en Cataluña era básicamente gratuito para Citizen Lab.

La participación de WhatsApp en la investigación en esta fase es mucho menos clara. Al parecer, WhatsApp se utilizó simplemente como justificación para lanzar la investigación y, tan pronto como reconocieron que había cinco políticos y activistas catalanes en su lista, se dejó de necesitarles. Por ejemplo, nadie parece haberles pedido que verificasen si los dispositivos de alguna de las otras 65 presuntas víctimas fueron pirateados en la violación de la seguridad de 2019.

*250/* *El Confidencial. Las dos grabaciones del iPhone del Villarejo catalán que destaparon la mafia de Tsunami. 1 de noviembre de 2020, https://www.elconfidencial.com/espana/2020-11-01/los-audios-en-el-iphone-del-villarejo-catalan-que-destaparon-la-corrupcion-de-tsunami_2814943/*

*ElDiario.es. Los audios de la supuesta trama rusa del procés: "Una cosa es que esté el estado soviético y otra es que sea una encerrona". 4 de noviembre de 2020, https://www.eldiario.es/catalunya/audios-supuesta-trama-rusa-proces-cosa-sovietico-sea-encerrona_1_6386021.html*

*El Periódico. Operación Volhov: Los audios de Víctor Terradellas con Xavier Vendrell y David Madí. 6 de noviembre de 2020, https://www.elperiodico.com/es/politica/20201103/victor-terradellas-xavier-vendrell-david-madi-audios-conversaciones-telefonicas-8187809*

Es difícil saber si en Cataluña se llevaron a cabo muchos análisis forenses en 2021, ya que Citizen Lab no ha compartido ningún registro sobre el trabajo de campo y los medios de comunicación no han cubierto este caso específico. Al año siguiente, una vez que Citizen Lab había recopilado pruebas suficientes para fundamentar la demanda de Apple contra NSO, se reactivó la investigación de CatalanGate.

El 10 de enero de 2022, el grupo secesionista de la sociedad civil Assemblea Nacional Catalana registró el dominio CatalanGate.cat.[251] Actualmente, la otra gran organización secesionista, Òmnium, es propietaria del dominio[252]. Esta página de propaganda acusa directamente a España de espionaje político y pide a los ciudadanos que presionen a la Comisión Europea para que inicie una investigación sobre España. Se publicó en inglés y catalán junto con el informe y mantiene al Sr. Antoni Comín como «víctima» pese a haber admitido que su nombre fue añadida a la lista de personas atacadas con Pegasus por error. La cuenta de Twitter denominada «@catalangate» cuenta con 182.600 seguidores y se ha utilizado durante años para promover campañas secesionistas de difamación contra España.

Según el libro del Sr. Torrent, el 15 de julio de 2020 el Sr. Maragall propuso la utilización del término «CatalanGate» para establecer un vínculo con el famoso caso de espionaje Watergate[253]. Sin embargo, este término no llegó al dominio público hasta la publicación del informe el 18 de abril de 2022. No está claro cómo estas organizaciones secesionistas descubrieron los resultados de la investigación antes de enero de 2022, a menos que participasen activamente en ella, como parecen corroborar los testimonios de los participantes. El Sr. Deibert afirma que «el personal del Citizen Lab decidió incluir el término en el título tras descubrir, poco antes de su publicación, que las víctimas utilizaban el término para referirse al caso»[254]. El uso de un título sesgado — CatalanGate: Extensive Mercenary Spyware Operation against Catalans using Pegasus and Candiru— que va más allá de las conclusiones del informe, no es un ejemplo de buena práctica académica. Este título intenta contribuir a crear un sentimiento de pánico moral omitiendo que el supuesto espionaje estuviera dirigido a políticos y activistas implicados en la campaña por una secesión unilateral ilícita.

*251/* *El Triangle. 'Catalangate', un muntatge propagandístic preparat al detall des de fa mesos. 22 de abril de 2022, https://www.eltriangle.eu/2022/04/22/catalangate-un-muntatge-propagandistic-preparat-al-detall-des-de-fa-mesos/*

*252/* *Catalangate.cat. Privacitat. https://catalangate.cat/privacitat/#privacitat*

*253/* *Torrent (2021) Pegasus, página 80.*

*254/* *Carta de Mr Ronald Deibert a Jordi Cañas, página 7.*

Además, el Sr. Deibert ha contribuido a alimentar la indignación en la esfera pública:

«Este informe no se limita al espionaje de los políticos catalanes. Se trata de una historia sobre el uso extenso y desproporcionado de las tecnologías de vigilancia, presuntamente por parte de una o más agencias del Gobierno español. Es una crisis democrática en este país».[255]

Esta declaración hiperbólica basada en un informe no revisado por pares, elaborado junto con un activista político sin experiencia en la investigación y que afirmaba ser víctima en el mismo informe está más cerca de un ejercicio de activismo político que de cualquier tipo de publicación académica. ¿Dispone de pruebas que demuestren que el presunto espionaje de los líderes secesionistas en España era «desproporcionado»? En Twitter, el Sr. Deibert también ha adoptado una actitud partidista en relación con el tema (véanse los tweets más adelante). El 24 de mayo de 2022, la representante de Asuntos Exteriores de la Generalitat visitó Canadá y, tras una reunión con el Sr. Deibert, afirmó que las 65 presuntas víctimas del espionaje son solo «la punta del iceberg» del caso CatalanGate.[256] Este tipo de mensaje alarmista, que encaja con la narrativa nacionalista, no ha sido corroborado por ninguna otra revelación pública por parte de Citizen Lab meses después.

255/ *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-usan-pegasus-porque-tienen-apetito-de-espiar.html

256/ *ElNational.cat. Alsina se reúne con el director de CitizenLab: "El CatalanGate es la punta del iceberg". 24 de mayo de 2022,* https://www.elnacional.cat/es/politica/alsina-reune-director-citizenlab-catalangate-punta-iceberg_762414_102.html

profdeibert retweeted

**Elies Campo**
@elies

"In Catalonia, everyone and their mother was hacked with Pegasus"

(Yes, my mother was hacked too)

A **@NewYorker** Radio Hour podcast followup to **@RonanFarrow's** investigation into mercenary spyware abuses.
With **@jcuixart** & **@TxellBonet**

23 de abril

**profdeibert**
@RonDeibert

A familiar plot in Spain from other cases in which **@citizenlab** has published evidence-based reports of **#pegasus** abuse:

First, deny & smear
Then, a gruding partial admission
Then, try to rationalize with dubious justifications

irishtimes.com/news/world/eur... via **@IrishTimes**

irishtimes.com
**Spanish premier faces crunch economic vote amid anger over spyi...**

**profdeibert**
@RonDeibert

Spanish PM says secret service needs reform after Pegasus scandal

But he also questions @citizenlab methods. Strangely, no one from Spanish gov has requestes to meet with us to validate

He must be getting his intel from the kooks on Twitter.

**Europa Press** @europapress

Sánchez dice que desconocía el espionaje a independentistas y cuestiona la metodología del informe de Citizen Lab.

No resulta ninguna sorpresa, pues, que los políticos nacionalistas también hayan participado activamente en una intensa campaña de propaganda tanto a nivel nacional como internacional. Se han instrumentalizado artículos de prensa,[257] vídeos,258 entrevistas,[259] documentales,[260] mesas redondas,[261] debates,[262] actividades de gestión de fondos,[263] e incluso discursos en festivales públicos[264] para criticar la operación ilegal de espionaje de Pegasus por parte de España y la represión que Citizen Lab habría presuntamente descubierto.

257/ *p. ej. , Vilaweb. Crónica de l'assalt al móbil de dos prestigiosos metges catalans amb Pegasus, 21 de abril de 2022, https://www.vilaweb.cat/noticies/catalangate-metges-elies-campo-maria-cinta-cid-pegasus/*

258/ *p. ej. , Assamblea. #CatalanGate. YouTube. 26 de abril de 2022, https://www.youtube.com/watch?v=JwHiZBMsu4U*

259/ *p. ej. , El Nacional.cat. Saskia Bricmont, MEP: "Spain tried to silence the victims of Catalangate", 5 de diciembre de 2022, https://www.elnacional.cat/en/politics/saskia-bricmont-mep-interview-pegasus-spain-silence-victims-catalangate_929562_102.html*

260/ *p. ej. , CCMA.cat. Pegasus, l'espia a la butxaca. 10 de octubre 2022, https://www.ccma.cat/tv3/30-minuts/pegasus-lespia-a-la-butxaca-a-30-minuts/noticia/3177895/*

261/ *p. ej. , FES Acatlán. UNAM. Facebook. Mesa redonda sobre el caso de espionaje masivo #CatalanGate. 27 de mayo de 2022, https://www.facebook.com/unamacatlan/videos/517790730094535; Club Suisse de la Press, Human Rights and New Technologies. Illegal surveillance as a global challenge to democracy, human rights and its impact on civil society: the Catalangate case, 30 de junio de 2022*

262/ *p. ej. , Assemblea. Facebook. Catalangate — Ejemplo de ciberespionaje masivo con Pegasus contra una ideología. 12 de octubre de 2022, https://www.facebook.com/events/493684142618782/?ref=newsfeed*

*Club Suisse de la Presse. Human Rights and New Technologies. Illegal surveillance as a global challenge to democracy, human rights and its impact on civil society: the Catalangate case. 30 de junio de 2022, https://pressclub.ch/human-rights-and-new-technologies-illegal-surveillance-as-a-global-challenge-to-democracy-human-rights-and-its-impact-on-civil-society-the-catalangate-case/*

263/ *p. ej. , Òmnium. CatalanGate: Democràcia Vigilada. Fes un Donatiu! https://catalangate.Òmnium.cat/*

264/ *El Mundo. Participación de las Naciones Unidas en el Tsunami Democràtic pregona las fiestas de Sants: «El Catalangate es el caso global más grande de espionaje digital». 20 de agosto de 2020, https://www.elmundo.es/cataluna/2022/08/20/63013533e4d4d803538b45eb.html*

**Òmnium Cultural**
@Òmnium

**@omniumintl** portem la denúncia del **#Catalangate** a la seu de l'ONU de Ginebra conjuntament amb ONG de defensa dels drets humans com **@institut_IDHC, @FrontLineHRD, @omctorg** i **@demsoc**

Segeuix-ho en directe: **pressclub.ch/human-rights-a...**

30 de junio

**Amnistia Internacional Catalunya**
@AmnistiaCAT

Noves revelacions de **@citizenlab** confirmades per Amnistia Internacional revelen que aquestes persones van ser espiades a Catalunya pel sistema Pegasus de NSO group:

- Elisenda Paluzie
- Sònia Urpí Garcia
- Txell Bonet
- Jordi Sànchez

**30 minuts**
@30minuts

"En el cas del **@catalangate, @citizenlab** va defensar amb fermesa que hi hagués una investigació independent. La comissió de secrets oficials de la directora del CNI és teatre!"
**@RonDeibert**

**#PegasusTV3**
**tv3.video/30mPegasus**

3:59 · 22 de diciembre de 2017

La presunta víctima Jordi Sànchez afirmó que este era «el mayor caso de espionaje en Europa en los últimos 50 años». La cuenta oficial de JxCat lo denominaba «el mayor caso de ciberespionaje jamás certificado». Diana Riba afirmó en una audiencia del Consejo de Europa que «el Estado español tiene un claro interés a la hora de saber cuáles son nuestras estrategias políticas y jurídicas en cualquier momento y utilizará cualquier sistema a cualquier precio para obtener esta información, no le importa si viola algún tipo de derecho político, Estado de Derecho o derechos humanos». Esta enérgica acusación parece contradecir el amplio consenso académico que considera a España como democracia que respeta el Estado de Derecho, y no parece reflejar una postura matizada o rigurosa que normalmente se esperaría de alguien que actuara como vicepresidenta de una comisión de investigación que habla en una audiencia pública formal en otra organización internacional.

El informe CatalanGate es la piedra angular de una campaña de comunicación internacional para desacreditar a España como democracia y justificar la independencia catalana. La forma en que los resultados se presentan en el informe y la forma en que han sido difundidos por Citizen Lab y los participantes en el estudio parecen confirmar que esta investigación no fue dirigida por un interés puramente académico y fue concebida y ejecutada para justificar una única hipótesis que era la más conveniente para el movimiento nacionalista catalán: el espionaje ilegal por parte de España. Como se explica más adelante, el calendario del informe parece haber sido escogido para mitigar el impacto negativo en el movimiento secesionista de algunas revelaciones relativas a su conexión con Rusia, la apropiación indebida de fondos públicos y la organización de actividades ilegales, en 2018 y 2019, para cuestionar el control español de Cataluña. En marzo de 2022, el apoyo a independencia cayó hasta su nivel más bajo desde 2014; el 38,8 %, y el nivel de movilización también había disminuido considerablemente. La campaña CatalanGate tenía por objeto alimentar la indignación y el descontento y revitalizar así un movimiento independentista en declive.

265/ *Jordi Sànchez. @jordisanchezp. Twitter. 18 de abril de 2022, https://twitter.com/jordisanchezp/status/1516016406642536451?s=20&t=0qndZNQDB-kOU1wCwymi5Q*

266/ *Junts per Catalunya. @JuntsXCat. Twitter. 18 de abril de 2022, https://twitter.com/JuntsXCat/status/1516008971500507144?s=20&t=0qndZNQDB-kOU1wCwymi5Q*

267/ *PACE audiencia pública. Min 24.*

268/ *El País. El apoyo a la independencia de Cataluña se desploma al 38%. 17 de marzo de 2022, https://elpais.com/espana/catalunya/2022-03-17/el-apoyo-a-la-independencia-de-cataluna-se-desploma-al-38.html*

# 11

# ¿El espionaje de Pegasus como herramienta para invalidar los procesos judiciales?

Inmediatamente después de la publicación del informe Catalan-Gate, todos los partidos y organizaciones secesionistas pusieron en marcha una sólida campaña de comunicación política. También emprendieron una serie de acciones judiciales, en su mayoría, pero no exclusivamente, contra los creadores de Pegasus en diferentes tribunales de justicia europeos. Desde entonces, un argumento fundamental que expresaron en las entrevistas con los medios de comunicación fue que el supuesto espionaje había afectado a varios abogados que defendían a líderes secesionistas ante los tribunales. Esto supondría una vulneración de los derechos de los acusados y su intención era solicitar la anulación de sus juicios y sentencias.[269]

269/ *El Mundo. El Independentismo usa el espionaje de Pegasus como ofensiva judicial, política y social contra el Estado. 25 de abril de 2022, https://www.elmundo.es/cataluna/2022/04/25/6265984dfc6c832c778b45cd.html*

El 14 de julio de 2020, cuando no se había confirmado ninguna infección en ninguno de los teléfonos de los políticos catalanes supuestamente espiados, el periodista de El País, Joaquín Gil, afirmó lo siguiente en un artículo:

## «Durante el tiempo en que el teléfono móvil de Torrent fue objetivo de Pegasus (2019), el líder independentista participó en docenas de reuniones políticas y testificó ante el Tribunal Supremo en el juicio de El Procés».[270]

En una entrevista en TV3, el 30 de abril de 2022, la periodista Sra. Cristina Puig preguntó en varias ocasiones al Sr. Gonzalo Boye si el supuesto espionaje de abogados podría servir para anular los casos de líderes partidarios de la independencia, y el Sr. Boye alegó que disponían de pruebas periciales que demostraban que habían sido espiados —presumiblemente refiriéndose al análisis de Citizen Lab— y anunció que emprenderían acciones legales ante distintos tribunales en relación con el derecho a la defensa de sus clientes.[271] Es sorprendente que incluso antes de que el escándalo en Cataluña se hiciera público, pero poco después de que el Gobierno español hubiera declarado estar investigando a Tsunami Democràtic, el Sr. Boye ya hubiese afirmado en Twitter que se había espiado a sus abogados con Pegasus.[272] Un año después, y meses después de que The Guardian y El País pu-

270/ *«Procés» se refiere al proceso político que los partidos partidarios de la independencia se habían comprometido a alcanzar la independencia unilateral. 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

271/ *CCMA.cat. TV3. Preguntes freqüents. Gonzalo Boye: "Hem sigut espiats i hi ha proves". 30 de abril de 2022.* https://www.ccma.cat/tv3/alacarta/preguntes-frequents/gonzalo-boye-hem-sigut-espiats-i-hi-ha-proves/video/6156598/

272/ *Gonzalo Boye. @boye_g. Twitter. 9 de noviembre de 2019,* https://twitter.com/boye_g/status/1193228293316730880?s=20

blicasen el escándalo, supuestamente su móvil fue atacado con Pegasus, según el informe de CatalanGate.

Citizen Lab modificó el contenido del informe CatalanGate en varias ocasiones tras su publicación el 18 de abril de 2022. Los informes de actualización no son completamente inusuales; sin embargo, en la investigación científica se espera que los cambios posteriores a la publicación se hagan explícitos y justificados. La más problemática de estas modificaciones fue el adelanto de la fecha de infección del Sr. Van Den Eynde del 14 de junio al 14 de mayo de 2020, sin reconocer este hecho en ningún registro de publicación (véase el cuadro 3).

Según el testimonio del Sr. Van Den Eynde en la Comisión PEGA el 28 de noviembre de 2022, muchas de las comunicaciones interceptadas eran entre «cliente y abogado o abogado-abogado» y «recibieron el mismo SMS de la Seguridad Social española que otras víctimas habían recibido, por lo que todas ellas, hasta 65 por ahora, han recibido ese SMS malicioso». Es más, afirma que «el mismo día que fui atacado (14 de mayo de 2020) o en torno a esa fecha, tuve una reunión, una reunión por vídeollamada, creo con quizá diez abogados que estaban debatiendo nuestra estrategia jurídica en el caso de los políticos catalanes encarcelados»[273] Por lo tanto, la nueva fecha de infección «actualizada» podría ser utilizada por el Sr. Van Den Eynde como argumento para intentar impugnar la sentencia judicial en dichos juicios.

Del mismo modo, la Sra. Diana Riba, presunta víctima y vicepresidenta de la Comisión de Investigación PEGA, alegó en una audiencia celebrada en el Consejo de Europa el 12 de diciembre de 2022 que fue presuntamente espiado en dos ocasiones cuando se reunió con juristas para debatir la estrategia jurídica en relación con los juicios del Sr. Oriol Junqueras, en julio y octubre de 2019[274]. Es curioso que las víctimas pretendan conocer con precisión el momento de sus infecciones cuando el informe solo menciona fechas aproximadas.

*273/* *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/pega-committee-meeting_20221129-0900-COMMITTEE-PEGA*

*274/* *PACE public hearing: Pegasus and similar spyware and secret state surveillance. Youtube. 12 de diciembre de 2022. https://www. youtube.com/watch?v=zZft_l0cWJs. Este testimonio parece contradecir el informe de «CatalanGate» en el que se dice que ella solo fue infectada en octubre de 2019.*

# 12

# Conexiones con Rusia y la estrategia de blockchain para la secesión

A pesar de las conexiones conocidas de varios de los participantes con los emisarios del Kremlin, el informe CatalanGate no hace ninguna referencia a Rusia y no considera que los servicios secretos rusos ni los piratas informáticos rusos puedan estar detrás de ninguna de las infecciones que afirman haber detectado en España, una hipótesis verosímil que Citizen Lab optó por descartar. Casualmente, las últimas rondas de análisis del informe CatalanGate fueron realizadas por Citizen Lab poco después de que surgieran varias pruebas incriminatorias de las investigaciones judiciales relativas a las relaciones entre líderes secesionistas y Moscú, y la aprobación en el Parlamento Europeo de una propuesta para investigar los vínculos entre el secesionismo catalán y Rusia en marzo de 2022.[275]

Organized Crime and Corruption Reporting (OCCR) publicó documentos que confirman y amplían las conexiones entre varios participantes en el trabajo de recogida de información y el análisis forense preliminar para el proyecto (y no reconocidos como tales), y los servicios secretos rusos[276] para desestabilizar España y la UE.[277] Las audiencias judiciales en España confirman también estos vínculos. La prensa nacional e internacional reflejó repetidamente esta aparente relación de colaboración entre líderes catalanes favorables a la independencia y Rusia durante el período de investigación. Sin embargo, este punto potencialmente relevante se omitió en el informe. Es bien sabido que los piratas informáticos rusos se habían inmiscuido en las instituciones españolas[278] y que promovieron el referéndum ilegal de independencia de 2017 habilitando sitios web alternativos para páginas prohibidas por la policía española[279] y a través de una campaña de desinformación.[280] Por ejemplo, entre el 11 y el 27 de septiembre de 2017, Sputnik publicó 220 *stories* sobre la crisis catalana y RT 85; existen pruebas de operaciones de amplificación de bots rusos, los mismos bots que amplificaron los mensajes en apoyo del Kremlin y el separatismo en Ucrania.[281] En febrero de 2019, las presuntas víctimas Josep Lluis Alay y Joaquim Torra difundieron un artículo de Komosomolskaya Pravda en el que se solicitaba la mediación de Moscú en la resolución del conflicto catalán.[282] En diciembre de 2019, piratas informáticos rusos piratearon el canal de televisión público español Canal 24 Horas para emitir una entrevista con el Sr. Puigdemont; el Sr. Sam Jones informó de ello en The Guardian, que[283] meses más tarde advirtió al Sr. Torrent de que estaba siendo espiado, y lo hizo presumiblemente en nombre de Citizen Lab.

*275/* *El País. El Parlamento Europeo cree necesario investigar los lazos entre Rusia y el independentismo catalán. 9 de marzo de 2022, https://elpais.com/espana/2022-03-09/el-parlamento-europeo-cree-necesario-investigar-los-lazos-entre-rusia-y-el-independentismo-catalan.html*

*276/* *OCCRP. Catalan Separatists Tailored Public Messaging to Avoid Antagonizing Russia: 'You Have to Avoid Navalny For Sure', 3 de septiembre de 2021, https://www.occrp.org/en/investigations/catalan-separatists-tailored-public-messaging-to-avoid-antagonizing-russia-you-have-to-avoid-navalny-for-sure*

277/ *OCCRP. Fueling Secession, Promising Bitcoins: How a Russian Operator Urged Catalonian Leaders to Break With Madrid, 8 de mayo de 2022, https://www.occrp.org/en/investigations/fueling-secession-promising-bitcoins-how-a-russian-operator-urged-catalonian-leaders-to-break-with-madrid*

278/ *El Confidencial. La Inteligencia española sospecha que Rusia estuvo tras el ciberataque al SEPE, 21 de marzo de 2021, https://www.elconfidencial.com/espana/2021-03-21/rusia-hackeo-sepe-inteligencia-espana_3000291/*

*EPE. Ciberdelincuentes rusos tratan de tumbar el sistema informativo de varias universidades españolas, 26 de febrero de 2022, https://www.epe.es/es/espana/20220226/ciberdelincuentes-rusos-ataque-informativo-universidades-espana-13295390*

*Información sobre el Segu-Info. Grupo pro ruso Killnet «declara» la guerra a España e Italia. 13 de mayo de 2022, https://blog.segu-info.com.ar/2022/05/grupo-pro-ruso-killnet-declara-la.html?m=0*

279/ *El País. Russian "hackers" help keep banned Catalan referendum census site online, 28 de septiembre 2017, https://english.elpais.com/elpais/2017/09/28/inenglish/1506588970_026442.html*

280/ *Euronews. Se investiga si una unidad militar rusa alimentó la crisis en Cataluña, 22 de noviembre de 2019, https://es.euronews.com/2019/11/22/se-investiga-si-una-unidad-militar-rusa-alimento-la-crisis-en-cataluna*

281/ *Atlantic Council's Digital Forensic Research Lab. @DFRLab. #ElectionWatch: Russia and Referendums in Catalonia? Medium. 28 de septiembre 2017, https://medium.com/dfrlab/electionwatch-russia-and-referendums-in-catalonia-192743efcd76*

282/ *ElNacional.cat. Full article: 'Komsomolskaya Pravda' proposes Russia as Spain-Catalonia mediator. 10 de febrero de 2019, https://www.elnacional.cat/en/politics/komsomolskaya-pravda-russia-spain-catalonia-mediator_353457_102.html*

*Torra aplaude una «mediación» de Rusia para Cataluña, 11 de febrero de 2019, https://cronicaglobal.elespanol.com/politica/torra-aplaude-mediacion-rusia-cataluna_221115_102.html*

283/ *The Guardian. Russian interview with Carles Puigdemont airs on hacked Spanish TV, 17 de diciembre de 2019. https://www.theguardian.com/world/2019/dec/17/spanish-tv-hacked-to-run-interview-with-carles-puigdemont*

Citizen Lab debe de haber sido consciente de las operaciones de desestabilización rusa en España y Europa. No solo el Sr. Deibert reconoció que Rusia estaba detrás de un caso de piratería informática de alto nivel en los Estados Unidos en 2017,[284] sino que Citizen Lab publicó un informe en 2017 en el que se hacía referencia a una operación rusa de phishing en 39 países.[285] Es extraño que Citizen Lab, tras haber escrito sobre las acciones de ciberespionaje ruso en Occidente en 2017, y conocedor de las conexiones entre Rusia y líderes secesionistas que se habían hecho públicas en varios medios de comunicación, ni siquiera considerara que Rusia podría haber tenido interés en espiar a los líderes catalanes con los que trataba, o incluso apoyarlos técnicamente en caso de que pudieran estar interesados en presentar a España como un país represivo que espía a sus ciudadanos. Es difícil discernir las razones por las que Citizen Lab descartó la participación rusa, o la de cualquier otro servicio secreto occidental preocupado por sus intentos de desestabilizar a los Estados Miembros de la UE. En el informe no se justifica la omisión de estas hipótesis.

En su carta a los diputados al Parlamento Europeo del Grupo Renew, el Sr. Deibert afirma que el Citizen Lab tuvo conocimiento de las acusaciones relativas a la colaboración de líderes secesionistas catalanes con los servicios de seguridad rusos en otoño de 2021. Sin embargo, la cobertura internacional por parte de la prensa del apoyo ruso al movimiento secesionista catalán se remonta al menos a 2017. Por ejemplo, este vínculo fue denunciado por titulares bastante explícitos en Politico («el referéndum catalán teme la influencia rusa»),[286] The Washington Post («Cataluña celebró un referéndum. Rusia ganó»)[287] El País («La maquinaria de injerencias rusa penetra la crisis catalana»),[288] BBC News Spain («Cataluña: ¿Echaron leña al fuego las *Fake News* rusas?»)[289] otros medios de comunicación también informaron de este enlace más adelante, como The New York Times («Matrimonio de espías del Kremlin, una misión opaca a Moscú y disturbios en Cataluña»),[290] Centre for European Policy Analysis («Cataluña: Donde hay problemas está Rusia»),[291] y The Times («Separatistas catalanes acusados de buscar ayuda de Rusia»).[292]

*284/* *Ronald Deibert (2017) The DHS/FBI Report on Russian Hacking was a Predictable Failure, Just Security, 4 de enero de 2017, https://www.justsecurity.org/35989/dhsfbi-report-russian-hacking-predictable-failure/*

*285/* *Adam Hulcoop, John Scott-Railton, Peter Tanchak, Matt Brooks, and Ron Deibert (2017). Tainted Leaks Disinformation and Phishing With a Russian Nexus. Citizen Lab 25 de mayo de 2017. https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/*

*286/* *Politico. Catalan referendum stokes fears of Russian influence, 29 de septiembre de 2017, https://www.politico.eu/article/russia-catalonia-referendum-fake-news-misinformation/*

287/ *The Washington Post. Catalonia held a referendum. Russia won. 2 de octubre de 2017, https://www.washingtonpost.com/opinions/global-opinions/catalonia-held-a-referendum-russia-won/2017/10/02/f618cd7c-a798-11e7-92d1-58c702d2d975_story.html*

288/ *El País. Russian meddling machine sets sights on Catalonia. 28 de septiembre de 2017, https://english.elpais.com/elpais/2017/09/26/inenglish/1506413477_994601.html*

289/ *BBC News. Spain Catalonia: Did Russian 'fake news' stir things up?, 18 de noviembre de 2017, https://www.bbc.com/news/world-europe-41981539*

290/ *The New York Times. Married Kremlin Spies, a Shadowy Mission to Moscow and Unrest in Catalonia, 3 de septiembre de 2021, https://www.nytimes.com/2021/09/03/world/europe/spain-catalonia-russia.html*

291/ *CEPA. Catalonia: Where There's Trouble There's Russia. 27 de septiembre de 2021, https://cepa.org/article/catalonia-where-theres-trouble-theres-russia/*

292/ *The Times. Catalan separatists accused of seeking Russia's help. 4 de septiembre de 2021. https://www.thetimes.co.uk/article/catalan-separatists-accused-of-seeking-russias-help-bp5dgdqg6*

Resulta sorprendente que Citizen Lab no refleje esta relación documentada en ninguna parte del informe. Ni siquiera en el relato sobre el referéndum de 2017. Citizen Lab también sugiere que quienes fueron investigados debido precisamente a sus conexiones con los servicios secretos rusos para desestabilizar España e independizarse son presuntas víctimas del espionaje «ilegal». ¿No deberían los servicios de securidad en las democracias investigar los intentos de subvertir el orden constitucional y su integridad territorial?

Según el proyecto OCCR, un representante de Putin se reunió con el presidente de la Generalitat, Carles Puigdemont,[293] el día anterior a la declaración unilateral de independencia de Cataluña en 2017. Se le prometieron 500.000 millones de dólares y 10.000 soldados si se comprometían a convertir Cataluña en un refugio de criptomonedas. Al parecer, esto formaba parte de una estrategia a largo plazo para erosionar la estabilidad del euro.[294] En 2016 y 2017 se documentaron varios viajes de agentes del GRU a Barcelona.[295] Varios de los participantes en el informe Citizen Lab trabajaron en la promoción de la tecnología de blockchain Ethereum (criptomoneda): el Sr. Campo, los Sres.

Miquel, Baylina, Escrich, Matamala, Ganyet y Vives. Al menos tres de los participantes en la investigación de Citizen Lab, el Sr. Alay,[296] el Sr. Boye[297] y la Sra. Artadi,[298] mantuvieron contactos con emisarios rusos en relación con el apoyo a una Cataluña independiente. En los años siguientes se celebraron varias reuniones con los emisarios de Putin en Suiza y Moscú.[299]

293/ *Carles Puigdemont y Clara Ponsetí afirman ser víctimas de la «persecución relacional» en el informe.*

294/ *OCCRP. Catalan Separatists Tailored Public Messaging to Avoid Antagonizing Russia: 'You Have to Avoid Navalny For Sure', 3 de septiembre de 2021, https://www.occrp.org/en/investigations/catalan-separatists-tailored-public-messaging-to-avoid-antagonizing-russia-you-have-to-avoid-navalny-for-sure*

295/ *El País. Tres espías de la unidad investigada viajaron a Barcelona en 2016 y 2017, 27 de diciembre de 2019, https://elpais.com/politica/2019/12/26/actualidad/1577390796_094918.html*

296/ *Confidencial. Los Contactos de Alay con los Rusos desatan una nueva crisis entre ERC y JxCAT. 16 de marzo de 2022, https://www.elconfidencial.com/espana/cataluna/2022-03-16/contactos-alay-rusos-crean-crisis-entre-erc-jxcat_3392350/*

297/ *El Confidencial. Los emisarios del Gobierno catalán habían viajado a Moscú hasta 2020 para obtener en secreto el apoyo de Putin. 14 de marzo de 2022, https://www.elconfidencial.com/espana/2022-03-14/emissaries-catalan-government-travelled-moscow_3390880/*

298/ *El Periódico. Puigdemont envió a Elsa Artadi a una reunión con rusos sobre criptomonedas antes de la DUI, 31 de mayo de 2022, https://www.elperiodico.com/es/politica/20220531/puigdemont-elsa-artadi-rusia-proces-13739860*

299/ *El Periódico. Carles Puigdemont, Rusia y el «procés»: 5 reuniones, 2 versiones. 24 de marzo de 2022, https://www.elperiodico.com/es/politica/20220327/puigdemont-alay-dmitrenko-rusia-cataluna-contactos-13431329*

*El Confidencial. La Generalitat pagó el primer viaje a Rusia del jefe de la oficina de Carles Puigdemont. 15 de marzo de 2022, https://www.elconfidencial.com/espana/cataluna/2022-03-15/generalitat-pago-viaje-hombre-puigdemont-rusia_3391758/*

Se sospechaba que activistas secesionistas, expertos en tecnología blockchain estaban colaborando con los servicios secretos rusos[300] en el diseño de Tsunami Democràtic,[301] una plataforma supuestamente dirigida por Xavier Vendrell[302], otro participante en el informe, actualmente investigado por la justicia. Tsunami Democràtic operaba a través de Telegram y contaba con una aplicación específica Android que se puso en marcha en octubre de 2019, el mismo mes que Citizen Lab se puso en contacto con el Sr. Miquel en varias ocasiones para notificarle de ataques con programas espía. El Sr. Miquel está siendo investigado actualmente por su participación en Tsunami Democràtic.[303] Este grupo se inspiró en una descentralización tipo blockchain y permitió el anonimato de sus participantes. Solo meses antes del inicio de la investigación «CatalanGate», los actos de sabotaje, los disturbios violentos y los bloqueos ilegales de carreteras, aeropuertos y estaciones de tren fueron coordinados a través de la aplicación Tsunami Democràtic, causando millones de euros en pérdidas y la muerte de un ciudadano francés en el aeropuerto de El Prat.[304] Hubo daños en las infraestructuras de transporte[305] y saqueos.[306] Por ejemplo, el sistema ferroviario de Barcelona sufrió diez sabotajes.[307] Incluso se produjo un ataque a un helicóptero policial que supervisaba los disturbios el 17 de octubre de 2019; esto podría haber causado un incidente mortal.[308]

*300/* *La Voz de Galicia. Un juez investiga si Rusia podría estar detrás de Tsunami Democrático, 3 de setiembre de 2021, https://www.lavozdegalicia.es/noticia/espana/2021/09/03/juez-investiga-rusia-estar-detras-tsunami-democratico/00031630666798801726366.html*

*Tiempo de Canarias. ¿Está la inteligencia rusa detrás de Tsunami Democràtic? 22 de noviembre de 2019. https://tiempodecanarias.com/esta-la-inteligencia-rusa-detras-de-tsunami-democratic*

*301/* *France 24. Clandestine 'tsunami' behind new wave of Catalan protests, 15 de octubre de 2019, https://www.france24.com/en/20191015-clandestine-tsunami-behind-new-wave-of-catalan-protests*

*302/* *El Periódico. El juez atribuye a Vendrell la dirección de Tsunami Democràtic. 28 de octubre de 2020, https://www.elperiodico.com/es/politica/20201028/xaver-vendrell-tsunami-democratic-juez-aguirre-8179456*

*303/* *El Confidencial. Tsunami usa los mismos proveedores de internet que las entidades de Puigdemont. 6 de noviembre de 2019, https://www.elconfidencial.com/espana/cataluna/2019-11-06/tsunami-proveedores-informaticos-puigdemont_2314724/*

304/ *EPE. El juez investiga en secreto la financiación de Tsunami Democràtic a través de cinco acciones. 4 de marzo de 2022, https://amp.epe.es/es/politica/20220304/juez-investiga-secreto-financiacion-tsunami-democratic-13325237*

*La Voz de Galicia. Muere un pasajero francés de un infarto durante el bloqueo secesionista en el aeropuerto de El Prat. 16 de octubre de 2019, https://www.lavozdegalicia.es/noticia/espana/2019/10/16/muere-pasajero-infartodurante-bloqueo-aeropuerto-prat/00031571228187505368503.htm*

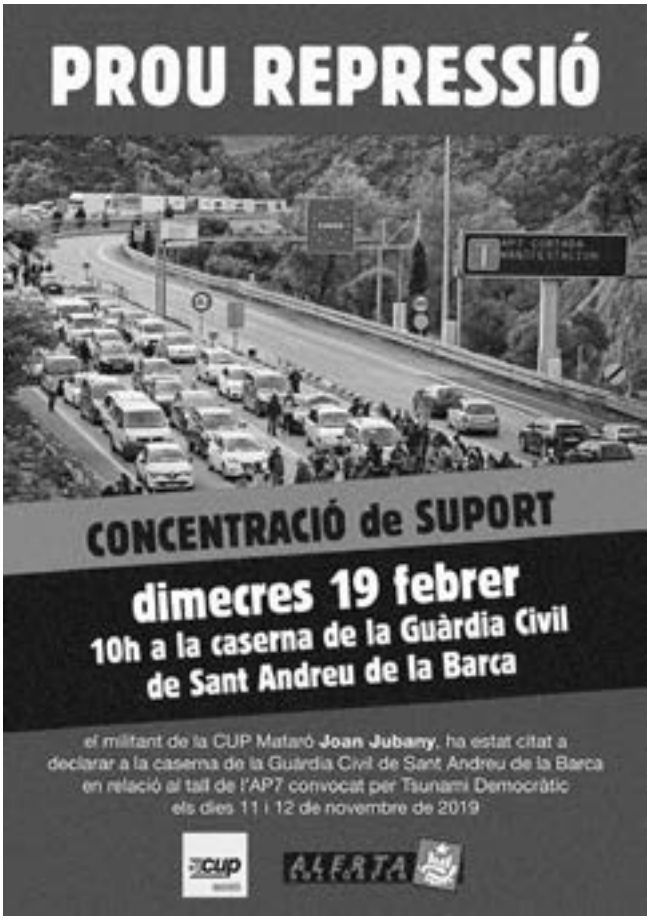
305/ *RTVE. Sentencia del 'procés' Fomento cifra en más de 7,3 millones de euros los daños en transporte e infraestructuras por las protestas en Cataluña, 23 de octubre de 2019, https://www.rtve.es/noticias/20191023/fomento-cifra-mas-73-millones-euros-perdidas-economicas-protestas-cataluna/1984581.shtml*

306/ *ABC. Los altercados de Barcelona derivan en pillaje y crean un «efecto llamada». 20 de octubre de 2019, https://www.abc.es/espana/abci-altercados-barcelona-derivan-pillaje-y-crean-efecto-llamada-201910202159_noticia.html*

307/ *El Periódico. Rodalies acumula una desena de sabotatges des de la sentència del judici del procés. 26 de octubre de 2019, https://www.elperiodico.cat/ca/politica/20191026/rodalies-acumula-una-desena-sabotatges-des-de-sentencia-judici-proces-7702383*

308/ *El Mundo. Así fue el ataque de los CDR al helicóptero de los Mossos en Barcelona. 17 de octubre de 2019, https://www.elmundo.es/cataluna/2019/10/17/5da816fb21efa008368b4581.html*

*Protestas en Gerona, 14 de octubre de 2019. Créditos: usuario de Wikipedia Davidpar. CC BY-SA 4.0*




*Créditos: imágenes de Twitter #tsunamidemocratic*

Al parecer, durante los años 2018 y 2019, varias de las presuntas víctimas mencionadas en el informe CatalanGate, como el Sr. Domingo, el Sr. Torra y el Sr. Ganyet, fueron investigadas por su participación en una operación de toma de control del territorio catalán en la que participaron grupos de activistas radicales de los Comités de Defensa de la República (CDR), así como algunos agentes de policía, guardas forestales y bomberos alineados políticamente.[309] Al parecer hubo planes para adquirir drones militares[310] y algunos de los activistas del CDR implicados estaban realizando pruebas de explosivos según informes policiales filtrados a la prensa.[311]

El 28 de octubre de 2020, las fuerzas policiales españolas detuvieron a 21 activistas secesionistas sospechosos de desvío de fondos públicos[312] para financiar el Tsunami Democràtic. Entre los detenidos había al menos tres de los participantes en la investigación de Citizen Lab: Josep Maria Alay, David Madi y Xavier Vendrell.[313] El 4 de noviembre de 2020, la prensa española publicó extractos de conversaciones interceptados[314] por la policía española entre el Sr. Victor Terradellas —hombre de negocios y amigo personal del Sr. Puigdemont y antiguo secretario de Asuntos Exteriores de Convergència Democràtica de Catalunya (CDC)— el Sr. Madi —político y empresario de la CDC— y el Sr. Vendrell —político de ERC y empresario, así como un antiguo miembro del grupo terrorista Terra Lliure[315]—. Los Sres. Terradellas y Madi hablan del interés de Rusia por las criptomonedas. La única condición de Rusia para apoyar a una Cataluña independiente era aprobar una legislación para adoptar un modelo descentralizado basado en la criptomoneda.[316]

El interés ruso en que Cataluña se convirtiese en un paraíso de criptomonedas, que piden a cambio de proporcionar su apoyo, resuena con las declaraciones públicas y los esfuerzos de muchos opositores nacionalistas y activistas en años posteriores. Por ejemplo, la presunta víctima, el Sr. Baylina, hace referencia al «sueño del pueblo catalán» y explica la estrategia para crear un nuevo Estado «descentralizado» basado en la tecnología blockchain que permitiría instituciones, «identidades autosoberanas» y pagos fuera del control de los Estados[317].

El relato del Sr. Baylina inspiró al del Sr. Puigdemont, a quien aconsejó al respecto. El Sr. Puigdemont va un paso más allá y declara «la obsolescencia de la democracia liberal tal y como la hemos entendido», sugiriendo que «los ciudadanos se organizan fuera de los Estados y crean sus propios sistemas en competencia o en sustitución de los que son específicos de los Estados, por ejemplo, la moneda o la criptomoneda»[318]. Hackers separatisatas catalanes fueron muy activos diseñando protocolos criptográficos para evitar los intentos de la policía española de neutralizar las páginas web usadas por los organizadores del referéndum ilegal (Poblet 2018).

El número de iniciativas de blockchain patrocinadas por el Gobierno y activistas secesionistas en Cataluña se multiplica después de 2017, al igual que sus reuniones con los emisarios del Kremlin. El 29 de octubre de 2017, The Asian Banker publicó en un artículo que «los criptográficos de Barcelona están siguiendo los consejos del experto en criptomonedas Vitalik Buterin, fundador de la plataforma blockchain Ethereum y programadores en Es-

tonia. La idea es crear una moneda fuera del control de España y del Banco Central Europeo».[320] Jordi Puigneró, político JxCat, antiguo vicepresidente y consejero regional de Políticas Digitales y Administración Pública, dirigió la estrategia nacionalista de construir una «nación digital en forma de república» o una «República Digital». Aunque «Cataluña no tiene control físico del territorio», esperaba crear «oportunidades» como las de los días 1 y 27 de octubre de 2017 para lograr la independencia de España.[321] El Sr. Puigneró explica que la idea surgió en noviembre de 2017 en una visita al Sr. Puigdemont, cuando demostró al antiguo presidente de Cataluña que era posible una vía digital hacia la independencia; a continuación, se le encargó la definición de un proyecto para un Estado digital.[322] Convertir a Cataluña en pionera de blockchain se convierte en la prioridad de la Generalitat de Catalunya en 2018.[323]

309/ *NIUS. La Guardia Civil acusa a Torra de planear una nueva Declaración Unilateral de Independencia en 2018 tras alentar disturbios en Cataluña. 19 de octubre de 2022, https://www.niusdiario.es/nacional/tribunales/20221019/guardia-civil-acusa-torra-independencia-unilateral-cataluna_18_07741742.html*

*El Confidencial. El CNI catalán creó un frente secretario de «Mossos», bomberos y guardas forestales para «controlar el territorio», 21 de octubre de 2022, https://www.elconfidencial.com/espana/2022-10-21/cataluna-independencia-cni-mossos-bomberos-guardas-territorio_3510022/*

310/ *El Confidencial. La Guardia Civil Conecta al CNI catalán con un plan militar con «drones de combate». 22 de octubre de 2022, https://www.elconfidencial.com/espana/2022-10-22/la-guardia-civil-dice-que-el-govern-planeo-hacer_3510532/*

311/ *El Mundo. La Guardia Civil concluye que los CDR detenidos formaban un grupo terrorista, 1 de noviembre de 2022, https://www.elmundo.es/espana/2022/11/01/63601370fdddffc6758b45cd.html*

312/ *El Confidencial. La Guardia Civil detiene a los empresarios que montaron Tsunami Democràtic. 28 de octubre de 2020. https://www.elconfidencial.com/espana/2020-10-28/la-guardia-civil-detiene-empresarios-lideres-tsunami-democratic_2808820/*

313/ *Europa Press. Detenidos Madí, Vendrell, Soler y Alay en una operación por presunto desvío de fondos al independiente. 28 de octubre de 2020, https://www.europapress.es/catalunya/noticia-detenidos-madi-vendrell-soler-alay-operacion-guardia-civil-contra-tsunami-democratic-20201028100853.html*

314/ *La Vanguardia. Los audios de la operación Vóljov. 4 de noviembre de 2020, https://www.lavanguardia.com/politica/20201104/49214825329/audios-operacion-volhov-david-madi-xavier-vendrell.html*

315/ *ABC. Vendrell confesó que otros militantes de Terra Lliure se integraron en ERC. 12 de mayo de 2006, https://www.abc.es/espana/abci-vendrell-confeso-otros-militantes-terra-lliure-integraron-200605120300-1421521987860_noticia.html*

316/ *Youtube. La Vanguardia. Los audios de la operación Vóljov. 4 de noviembre de 2020, https://www.youtube.com/watch?v=gQ9TlPnZ-xU*

317/ *Web3 Foundation. Youtube. Jordi Baylina Presents Building a new Decentralized State at Web3 Summit 2019. 20 de septiembre de 2019, https://www.youtube.com/watch?v=P2L-8ZqZ7CI&t=1s*

*Ether Cash. Get the Decentralized Revolution. 26 de diciembre de 2017, https://ethercash.wordpress.com/tag/jordi-baylina/*

318/ *La República Digital Catalana. YouTube con extractos de un discurso público de Carles Puigdemont en Eslovenia con Ivo Vajgl. 21 de mayo de 2020 https://www.youtube.com/watch?v=Z6uQZDP0C1Q*

319/ *Poblet, M. (2018). Distributed, privacy-enhancing technologies in the 2017 Catalan referendum on independence: New tactics and models of participatory democracy. First Monday. https://firstmonday.org/ojs/index.php/fm/article/view/9402*

320/ *El Punt Avui. Puigneró aposta per crear una «nació digital en forma de república» amb el desplegament del Consell de la República. 18 de agosto de 2018, https://www.elpuntavui.cat/politica/article/17-politica/1452154-puignero-aposta-per-crear-una-nacio-digital-en-forma-de-republica-amb-el-desplegament-del-consell-de-la-republica.html*

321/ *The Asian Banker. Catalans race to create new currency as independence counter-attacks builds. 29 de octubre de 2017, https://www.theasianbanker.com/press-releases/catalans-race-to-create-a-new-currency-as-independence-counter-attack-builds*

*ARA. Puigneró aposta per avançar cap a una República «digital» mentre Catalunya no tingui el control físic del territori. 18 de agosto de 2018, https://www.ara.cat/politica/puignero-construir-republica-catalunya-territori_1_2731212.html*

322/ *Puigneró, J. (2020). El 5è poder: La República Digital a les teves mans. La Campana.*

323/ *Decentral Blockchain & Cryptocurrency. Medium. 1 de agosto de 2018, https://medium.com/@DecentralEng/catalonia-a-pioneer-in-blockchain-implementation-211156c151ae*

En junio de 2019, el Gobierno catalán aprobó la estrategia de blockchain de Cataluña.[324] En agosto de 2020, la Generalitat creó la tecnología de blockchain de Cataluña,[325] en diciembre de 2020, el nuevo Centre Blockchain de Catalunya (CBCat) abre su sede en la Universidad de Girona; en enero de 2021, el Sr. Baylina y el Sr. Matamala pusieron en marcha la Fundació Nord;[326] y nuevas sucursales de CBCat se abrieron en Vic en septiembre de 2021[327]y en Badalona en octubre de 2022.[328] Al menos tres criptomonedas catalanas comenzaron a operar en Cataluña, aparentemente promovidas por partidos y activistas nacionalistas: Croat, CatalanCoin y Meal token.[329] Dado el fracaso de estos proyectos, los líderes secesionistas más tarde se manifestaron abiertamente a favor de Ethereum, la criptomoneda creada por el promotor ruso Vitalik Buterin.[330]

*324/* *Gencat. Estratègia de blockchain de Catalunya. Junio de 2019, https://smartcatalonia.gencat.cat/en/projectes/tecnologies/detalls/article/estrategia-blockchain-de-catalunya*

*325/* *eSmartcity.es. En marcha el Observatorio de Tecnologías Blockchain de Cataluña, 31 de agosto de 2021, https://www.esmartcity.es/2020/08/31/en-marcha-observatorio-tecnologias-blockchain-cataluna#.YpO0_crixe0.twitter*

*326/* *El Confidencial. El entorno de Puigdemont crea una fundación en Girona para impulsar criptomonedas, 3 de mayo de 2022, https://www.elconfidencial.com/espana/cataluna/2022-05-03/puigdemont-crea-fundacion-girona-criptodivisas_3417927/*

*327/* *Govern.cat. Vic, subseu del Centre Blockchain de Catalunya. 10 de septiembre de 2021, https://govern.cat/salapremsa/notes-premsa/413472/vic-subseu-del-centre-blockchain-catalunya*

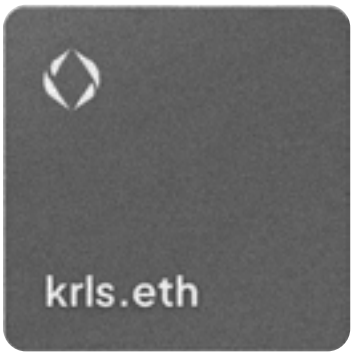
*328/* *LaVanguardia. El Centro Blockchain de Catalunya abre una subsede en Badalona. 26 de octubre de 2022, https://www.lavanguardia.com/local/barcelones-nord/20221026/8583219/centro-blockchain-catalunya-abre-subsede-badalona.html#:~:text=El%20CBCat%20(Centro%20Blockchain%20de,blockchain%20en%20el%20sector%20energ%C3%A9tico.*

*329/* *El Confidencial. Los independentistas se pelean por imponer la moneda virtual de la república catalana. 30 de diciembre de 2018, https://www.elconfidencial.com/espana/cataluna/2018-12-30/independentistas-pelea-imponer-moneda-virtual-republica-catalana_1708922/*

*ElEconomista.es. Casa Meal ultima el Lanzamiento de «Meal Token», la primera criptomoneda española asociada a una compañía productiva. 16 de enero de 2018, https://www.eleconomista.es/mercados-cotizaciones/noticias/8871049/01/18/Home-Meal-ultima-el-lanzamiento-de-Meal-Token-la-primera-criptomoneda-espanola-asociada-a-una-compania-productiva.html*

**krls.eth / Carles Puigdemont**
@KRLS

Des de fa un temps, gràcies a l'ajuda inestimable de veritables experts, valoro la potencialitat transformadora que la tecnologia té sobre la governança, l'organització política i les ideologies. No pas com a tecnòleg, que no en sóc, sinó com a responsable polític.




**krls.eth / Carles Puigdemont** @KRLS · 31 dic, 2021

El que es coneix com a Web3 està establint les bases d'una millor manera de servir la societat, basant-se en la privadesa, la seguretat i la transparència. Això permet construir el que algunes persones anomenen "estats descentralitzats".

youtube.com
**Jordi Baylina Presents Building a new Decentralized State at...**

**krls.eth / Carles Puigdemont** @KRLS · 31 dic, 2021

Això no és nou; durant el referèndum d'independència de l'1 d'octubre les tecnologies descentralitzades van ser usades per contrarestar la censura d'Espanya, com el sistema d'emmagatzematge distribuït **@ipfs.**

> **krls.eth / Carles Puigdemont** @KRLS · 23 Sep, 17
> No es poden posar portes al camp: en aquesta web trobaràs el lloc on et correspon votar l'1 d'octubre gateway.ipfs.io/ipns/QmZxWEBJB... **#1Oct**

**krls.eth / Carles Puigdemont** @KRLS · Dec 31, 2021

Aquesta nova generació de tecnologies descentralitzades va començar l'any 2008 quan Satoshi Nakamoto va inventar el Bitcoin, el primer sistema de pagament peer-to-peer i resistent a la censura en un registre distribuït.

**krls.eth / Carles Puigdemont** @KRLS · 31 dic, 2021

Al 2015, **@VitalikButerin** i altres desenvolupadors van crear la blockchain Ethereum, la primera cadena de blocs que permetia executar codi convertint-se en el primer ordinador distribuït i resistent a censura.

**krls.eth / Carles Puigdemont** @KRLS · 31 dic, 2021

Des de llavors, una explosió cambriana de protocols, infraestructures i productes ha atret i inspirat a tot el món, evitant els intermediaris i generant nous models de governança, identitat, propietat i financers.

**krls.eth / Carles Puigdemont** @KRLS · 31 dic, 2021

Des de fa segles, els grups culturals, associacions i cooperatives han estat un pilar bàsic de la societat catalana. Amb l'aparició de Web3, alguns d'ells evolucionen cap a DAOs, on el seu codi de governança és de codi obert i transparent.

**krls.eth / Carles Puigdemont** @KRLS · 31 dic, 2021

A més, Catalunya ha estat històricament pionera en els nous cicles tecnològics, ja sigui contribuint al desenvolupament o a l'adopció per part dels seus ciutadans. El que està passant a Web3 no serà diferent.

**krls.eth / Carles Puigdemont** @KRLS · 31 dic, 2021

Avui presento la meva cartera pública Ethereum krls.eth, amb la intenció de contribuir, experimentar i participar activament en la governança i perquè els governs serveixin millor als seus ciutadans.

**krls.eth / Carles Puigdemont**
@KRLS

La República a les teves mans.
Ja he rebut la targeta amb el QR de la meva Identital Digital Republicana
Demana-la ja al web del Consell i anem desconnectant de l'Estat
**#IDRepublicana #PreparemNos**
**consellrepublica.cat**

6:57 PM · 6 de abril de 2021

**Elisenda Paluzie**
@epaluzie

Com a membre en representació de l'**@assamblea** del Consell de Govern del **@ConsellxRep** ja he rebut la targeta amb el QR de la meva Identital Digital Republicana. Demana-la ja al web del Consell!
**#IDRepublicana #PreparemNos**
**consellrepublica.cat**

8:48 AM · 7 de abril de 2021

En las conversaciones telefónicas interceptadas por la policía, el Sr. Terradellas afirma estar en contacto con uno de los fundadores rusos de criptomonedas y que el Sr. Puigdemont le explicó en Waterloo todas las cosas que estaban haciendo con las criptomonedas.[331] El Sr. Madi menciona que tres equipos estaban trabajando en esta tarea. Mientras tanto, en el audio publicado del intercambio[332] entre el Sr. Terradellas y el Sr. Vendrell, también hay referencias explícitas a los 10.000 soldados rusos, al control del aeropuerto y otras infraestructuras y a la necesidad de «100 muertos» para justificar la participación rusa. El Sr. Terradellas alega que, si reunieran a 1 millón de personas en la plaza Sant Jaume (donde se encuentran el Gobierno catalán y el ayuntamiento), las fuerzas de seguridad españolas tendrían que matar a personas para entrar. El Sr. Vendrell afirma que perdieron la oportunidad,[333] y que no disponían de las agallas para hacerlo. El Sr. Terradellas añade que la situación mundial brindará una nueva oportunidad y que «Europa caerá». El Sr. Terradellas posteriormente confirmó en el tribunal[334] las conversaciones sobre posibles víctimas civiles y el hecho de que el Sr. Puigdemont no rechazó las ofertas de los emisarios del Kremlin y pidió que se siguiera debatiendo esta posibilidad con ellos.

*331/* *ElDiario.es. Los audios de la supuesta trama rusa del procés: "Una cosa es que esté el estado soviético y otra es que sea una encerrona". 4 de noviembre de 2020, https://www.eldiario.es/catalunya/audios-supuesta-trama-rusa-proces-cosa-sovietico-sea-encerrona_1_6386021.html*

**Elies Campo**
@elies

A new era begins for the **@ethereum** ecosystem. The **@eth2** Epoch 0 has been finalized. Congratulations!

**beaconcha.in/block/0**

12:11 · 1 de diciembre de 2020

**Jordi Pu1gnerO**
@jordiPuignero

"Los catalanes hacen cosas". Doncs sí. Avui hem presentat el llançament de la criptomoneda "Meal" de l'empresa Catalana **@nostrum_123**. La innovació digital d'una empresa de producte nacional és possible (i necessària) **#smartcat #blockchain @KRLS**

7:04 PM · 27 de diciembre de 2017

**Joan Canadell**
@jacanadellb

Tb es podran muntar eines q ja existeixen a la República digital d'Estonia i q us adjunto en imatge. Fizeu-vos amb e-banking, e-justice, e-Tax!!!... Tb podem innovar un sistema de voluntariat x la República, o qualsevol altre q connecti i millori la nostra vida >>>>

11:11 AM · 16 de diciembre de 2018

Follow

**Jordi Baylina - baylina.eth**
@jbaylina

Blockchain developer, Ethereum fan, white hat hacker and Catalonia Freedom fighter.

332/ *YouTube. Aussiesta. Terradellas y Vendrell dicen que hacen falta 100 Muertos para involucrar a Rusia (vídeo extraído de la cuenta de Twitter El Periódico), 4 de noviembre de 2020* https://www.youtube.com/watch?v=hLjmxaiwRjs

333/ *El Periódico. Operación Volhov: Los audios de Víctor Terradellas con Xavier Vendrell y David Madí. 3 de noviembre de 2020,* https://www.elperiodico.com/es/politica/20201103/victor-terradellas-xavier-vendrell-david-madi-audios-conversaciones-telefonicas-8187809

334/ *El Periódico. VIDEO | Víctor Terradellas, ante el juez: "Puigdemont no declinó la oferta de los rusos. Solo dijo: 'seguid hablando'". 20 de mayo de 2022,* https://www.elperiodico.com/es/politica/20220520/victor-terradellas-declaracion-integra-trama-rusa-proces-video-13682154

El Sr. Terradellas se reunió con los Sres. Puigdemont y Jordi Sardà el 26 de octubre de 2017 y, a raíz de dicha reunión, se decidió supuestamente ponerse en contacto con el líder ultranacionalista Vladimir Zhirinovsky.[335] El Sr. Zhirinovsky organizó posteriormente una concentración de apoyo al separatismo catalán, comparándola con los movimientos rusos secesionistas en Ucrania, ante el Consulado General de España en Moscú el 10 de noviembre de 2017.[336,337]

Si Citizen Lab sabía que los servicios secretos rusos podrían estar colaborando con alguno de los participantes mencionados y conocían las investigaciones judiciales formales contra ellos, en varios casos públicos desde 2020, ¿por qué siguieron considerándolos «víctimas del espionaje ilegal»? ¿Se han tomado precauciones especiales en relación con la colaboración con los Sres. Alay, Vendrell, Madi o Boye en la investigación? ¿Ningún organismo de Citizen Lab consideraba que los servicios secretos estadounidenses, británicos u otros servicios secretos occidentales pudieran estar interesados en espiar a activistas catalanes que pudieran colaborar con los servicios secretos rusos para desestabilizar la UE? Resulta sorprendente que en el informe no se mencione ninguno de los hechos e hipótesis antes mencionados. Ciertamente, debilitarían la ya muy superficial acusación contra España.

335/ *El Confidencial. El encuentro secreto de Artadi con un hombre de Gorbachov y Vladímir Putin en Barcelona, 29 de mayo de 2022, https://www.elconfidencial.com/espana/cataluna/2022-05-29/encuentro-secreto-artadi-gorbachov-putin-barcelona_3432185/?utm_source=twitter&utm_medium=social&utm_campaign=BotoneraWeb&s=09*

336/ *CountingStars. The Russian Nationalist Who Threatened to Raze Poland Now Supports Catalan Separatism. 11 de noviembre de 2017, https://www.outono.net/elentir/2017/11/11/the-russian-nationalist-who-threatened-to-raze-poland-now-supports-catalan-separatism/*

337/ *Captura de Youtube con subtítulos autogenerados en inglés. LDPR-TV. Митинг у Посольства Испании. Жириновский живьем от 10.11.2017. Youtube. https://www.youtube.com/watch?v=rFNyjBPoyno*

Dado que la información relativa a estos intentos de involucrar al ejército ruso en un esfuerzo separatista catalán se publicó en 2020, y que muchas grabaciones incriminatorias estaban ampliamente disponibles en línea, es sorprendente que Citizen Lab decidiera invitar a estas personas a formar parte de su estudio. Tampoco hay pruebas de que el Consejo de Investigación Ética de la Universidad de Toronto haya sido informado por Citizen Lab sobre la posible interacción con el trabajo legítimo de los servicios de seguridad españoles para defender al país contra una supuesta campaña rusa de desestabilización. A pesar de ser consciente de que muchas «víctimas» estaban siendo procesadas, y algunas por delitos graves, Citizen Lab decidió utilizar un lenguaje sensacionalista en el informe de CatalanGate, y sugirió que el seguimiento español era «sin restricciones, innecesario y desproporcionado»[338].

Citizen Lab afirma lo siguiente:

«Muchas de las víctimas no fueron acusadas de delitos graves y la mayoría no eran delincuentes ni, ciertamente, terroristas las justificaciones típicas que emplean las empresas de vigilancia mercenaria para vender sus programas espía a clientes gubernamentales».[339]

Esto significa que eran conscientes de que otras «víctimas» habían sido acusadas o investigadas formalmente por delitos graves. Así que, atribuirles el papel de «víctima» podría considerarse un ejercicio extremadamente problemático. ¿Por qué ha omitido Citizen Lab que varios de los participantes han sido objeto de una autorización judicial públicamente conocida (como los Sres. Madi y Vendrell)? Este tipo de hipótesis, opciones y limitaciones de investigación suelen reflejarse en la conclusión o en otro lugar de un informe. Lamentablemente, Citizen Lab optó por no reconocerlos.

*338/ Scott-Railton et al. (2022). CatalanGate, página 23*
*339/ Scott-Railton et al. (2022). CatalanGate, página 24.*

Además, el Sr. Boye, otro participante en el estudio y presunta víctima, fue nombrado abogado de dos presuntos espías rusos. Fue seleccionado para representar a D. Pablo González, periodista español detenido el 4 de marzo de 2022 en la frontera entre Polonia y Ucrania, sospechoso de ser un activo GRU,[340] y Anatoliy Shariy, bloguero prorruso detenido en España, acusado de alta traición y objeto de una orden de detención internacional solicitada por los servicios de seguridad de Ucrania el 5 de mayo de 2022.[341] Cabe señalar que el Sr. Boye es el abogado del Sr. Carles Puigdemont y ha representado a otras personalidades de alto prestigio, como Edward Snowden y el jefe narco «Sito Miñanco»[342]. Además, en 1996 fue condenado a 14 años de prisión acusado de terrorismo por ayudar a ETA a secuestrar a un empresario[343], y actualmente está siendo juzgado y se enfrenta a una posible condena de 9 años de prisión por lavado de dinero del narcotráfico.[344] El Sr. Boye fue una figura central en la elección de casos sospechosos dentro de las filas de JxCat[345] y en marzo de 2022, poco antes de la publicación del informe CatalanGate, se le conectó con Alexander Dmitrenko[346], un empresario y supuesto espía ruso[347] que vive en Cataluña y es un activista secesionista. Al Sr. Dimitrenko se le investigaba por organizar algunas de las reuniones entre emisarios rusos y líderes secesionistas.[348] Aunque su nombre no aparece en el informe[349], recientemente afirmó en Twitter que había sufrido 9 intentos de infección por Pegasus confirmados por el software de Amnistía Internacional,[350] El Sr. Boye también ha difundido información a favor de Kremlin y criticado a Ucrania desde la invasión.[351]

*340/* *New Straits Times. Poland detains Spanish reporter suspected of spying for Russia. 4 de marzo de 2022, https://www.nst.com.my/world/world/2022/03/776991/poland-detains-spanish-reporter-suspected-spying-russia*

*Público. Gonzalo Boye, abogado de Pablo González: «Es una situación incomprensible desde el punto de vista del derecho de la UE», 24 de marzo de 2022, https://www.publico.es/internacional/guerra-rusia-ucrania-gonzalo-boye-abogado-pablo-gonzalez-situacion-incomprensible-punto-vista-derecho-ue.html*

*341/* *Daily Mail. Ukrainian blogger accused of being a pro-Putin propagandist is arrested in Spain for 'high treason'. 5 de mayo de 2022, https://www.dailymail.co.uk/news/article-10785457/Ukrainian-blogger-accused-pro-Putin-propagandist-arrested-Spain.html*

*Europa Press. Pasa a disposición de la AN un bloguero prorruso detenido en Tarragona cuya defensa lleva el abogado de Puigdemont. 5 de mayo, https://www.europapress.es/nacional/noticia-pasa-disposicion-an-bloguero-prorruso-detenido-tarragona-cuya-defensa-lleva-abogado-puigdemont-20220505112958.html*

*342/* *Confilegal. Gonzalo Boye, abogado de Puigdemont, citado a declarar mañana como investigado por supuesto blanco vinculado a Sito Miñanco. 22 de octubre de 2019, https://confilegal.com/20191022-gonzalo-boye-abogado-de-puigdemont-citado-a-declarar-manana-como-investigado-por-supuesto-blanqueo-vinculado-a-sito-minanco/*

343/ *El Confidencial. El oscuro pasado de Boye, condenado por el secuestro de ETA a Emiliano Revilla. 21 de octubre de 2019, https://www.elconfidencial.com/espana/2019-10-21/boye-secuestro-eta-sito-minanco-registro_2292459/*

344/ *El Confidencial. La Fiscalía pide más de nueve años de CÁRCEL para el abogado de Puigdemont por blanqueo. 29 de noviembre de 2022, https://www.elconfidencial.com/espana/2022-11-29/abogado-puigdemont-boye-fiscal-carcel-minanco_3531600/*

345/ *Torrent (2022). Pegasus, página 142.*

346/ *El confidencial. Puigdemont se reunió en un hotel de Ginebra con el enlace del Kremlin, 15 de marzo de 2022.*

347/ *The Canadian News. Puigdemont's entourage commissioned inquiries into an alleged Russian spy. 10 de mayo de 2022, https://thecanadian.news/puigdemonts-entourage-commissioned-inquiries-into-an-alleged-russian-spy/*

*El País. Alexander Dmitrenko: «Es un Chiste que me halaga, pero no soy un espía». 30 de junio de 2022, https://elpais.com/espana/catalunya/2022-06-30/alexander-dmitrenko-es-un-chiste-que-me-halaga-pero-no-soy-un-espia.html*

348/ *El País. El juez CITA al empresario que abrió las puertas de Rusia al entorno de Puigdemont, 27 de abril de 2022, https://elpais.com/espana/catalunya/2022-04-27/el-juez-cita-al-empresario-que-abrio-las-puertas-de-rusia-al-entorno-de-puigdemont.html*

349/ *The «CatalanGate» se refiere a 4 víctimas anónimas cuya identidad no ha sido revelada.*

350/ *Alexander Dmitrenko. @alexdemitre. Twitter. 10 de mayo de 2022, https://twitter.com/alexdemitre/status/1523978375081205767?s=20&t=S4bss86nou16R7Qm-JQQiw*

*Alexander Dmitrenko. @alexdemitre. Twitter. 10 de mayo de 2022, https://twitter.com/alexdemitre/status/1523998269185134593?s=20&t=S4bss86nou16R7Qm-JQQiw*

351/ *Gonzalo Boye. @boye_g. Twitter. 3 de marzo de 2022, https://twitter.com/boye_g/status/1499260022680924161?s=20&t=6A-1NbPb0eY26SYm9Mk_eQ*

*Gonzalo Boye. @boye_g. Twitter. 11 de diciembre de 2022, https://twitter.com/boye_g/status/1602048655753728001?s=20&t=6A-1NbPb0eY26SYm9Mk_eQ ; 28 June 2022*

*Gonzalo Boye. @boye_g. Twitter. 28 de junio de 2022, https://twitter.com/boye_g/status/1541767629442109441?s=20&t=6A-1NbPb0eY26SYm9Mk_eQ*

*Gonzalo Boye. @boye_g. Twitter. 13 de marzo de 2022, https://twitter.com/boye_g/status/1502914757782867968?s=20&t=6A-1NbPb0eY26SYm9Mk_eQ*

*Gonzalo Boye. @boye_g. Twitter. 17 de febrero de 2022, https://twitter.com/boye_g/status/1494348820817326080?s=20&t=6A-1NbPb0eY26SYm9Mk_eQ*

*Gonzalo Boye. @boye_g. Twitter. 17 de febrero de 2022, https://twitter.com/boye_g/status/1494197314113744896?s=20&t=6A-1NbPb0eY26SYm9Mk_eQ*

**Gonzalo Boye**
@boye_g

Però els ucraïnesos són nazis o no?

vilaweb.cat
**Però els ucraïnesos són nazis o no?**

**Gonzalo Boye**
@boye_g

Entrevista | Wolfgang Kaleck, abogado de Snowden: “Hay evidencias de torturas de civiles en Ucrania, pero ahora falta probar su responsable penal”
20minutos.es/noticia/507892... vía **@20m**

20minutos.es
**Entrevista | Wolfgang Kaleck, abogado de Snowden: “Hay evidencias de tortu...**

10:12 PM · 11 de diciembre de 2022

**Gonzalo Boye**
@boye_g

Un interesante análisis:

No es verdad que Rusia esté cometiendo errores militares en Ucrania

elconfidencial.com
**No es verdad que Rusia esté cometiendo errores militares en Ucrania**

8:49 AM · 13 de marzo de 2022

**Gonzalo Boye**
@boye_g

¿De verdad?

Borell dice que en Rusia ha iniciado “intensos bombardeos” en el este de Ucrania

elespanol.com
**Borell dice que en Rusia ha iniciado “intensos bombardeos” en el este de Ucrania**

5:31 PM · 17 de febrero de 2020

**Gonzalo Boye** ✓
@boye_g

Veo que en Ucrania también persiguen a los abogados de los opositores...

> **@anatoliisharii** ✓ Jun 28
> In order to prevent us from defending ourselves in court after the illegal ban of a political party, a criminal case was also opened against our lawyer. For a RUDE ANSWER TO the SBU INVESTIGATOR in correspondance!!!! What a nice European country.

2:57 PM · 28 de junio de 2022

**Gonzalo Boye** ✓
@boye_g

Rusia pide a occidente un calendario de invasiones para poderse organizar con tiempo las vacaciones noticiasdenavarra.com/actualidad/pol... vía **@noticiasnavarra**

5:31 PM · 17 de febrero de 2020

Josep Lluís Alay, jefe de personal del Sr. Puigdemont, es una de las presuntas víctimas de CatalanGate que, en repetidas ocasiones, ha sido relacionada con los servicios secretos rusos, y supuestamente viajó con frecuencia a Moscú para obtener en secreto el apoyo del Kremlin. El Sr. Alay ha expresado públicamente su fascinación por los espías rusos y soviéticos y se ha reunido con algunos de ellos personalmente.

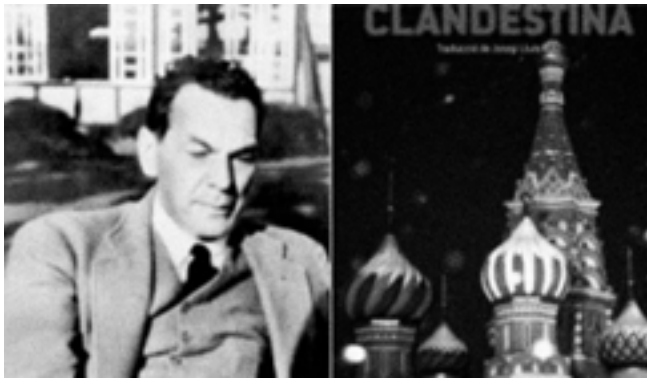
**Josep Lluís Alay**
@josepalay

En **@vpartal** comenta avui al seu editorial: 'Ahir vaig poder parlar llargament amb Elena Vavilova, l'espia russa que durant vint-i-cinc anys va viure com a agent il·legal del KGB dins els Estats Units. Té una història fascinant, absolutament increïble..."
**vilaweb.cat/noticies/ofega...**

22 de abril de 2021

**Josep Lluís Alay**
@josepalay

El gran espia soviètic de la Segona Guerra Mundial, Richard Sorge, molt proper a l'espia Ursula Kuczynski, també apareix a la novel·la 'El secret de la clandestina' d'**@E_VavilovaFoley**

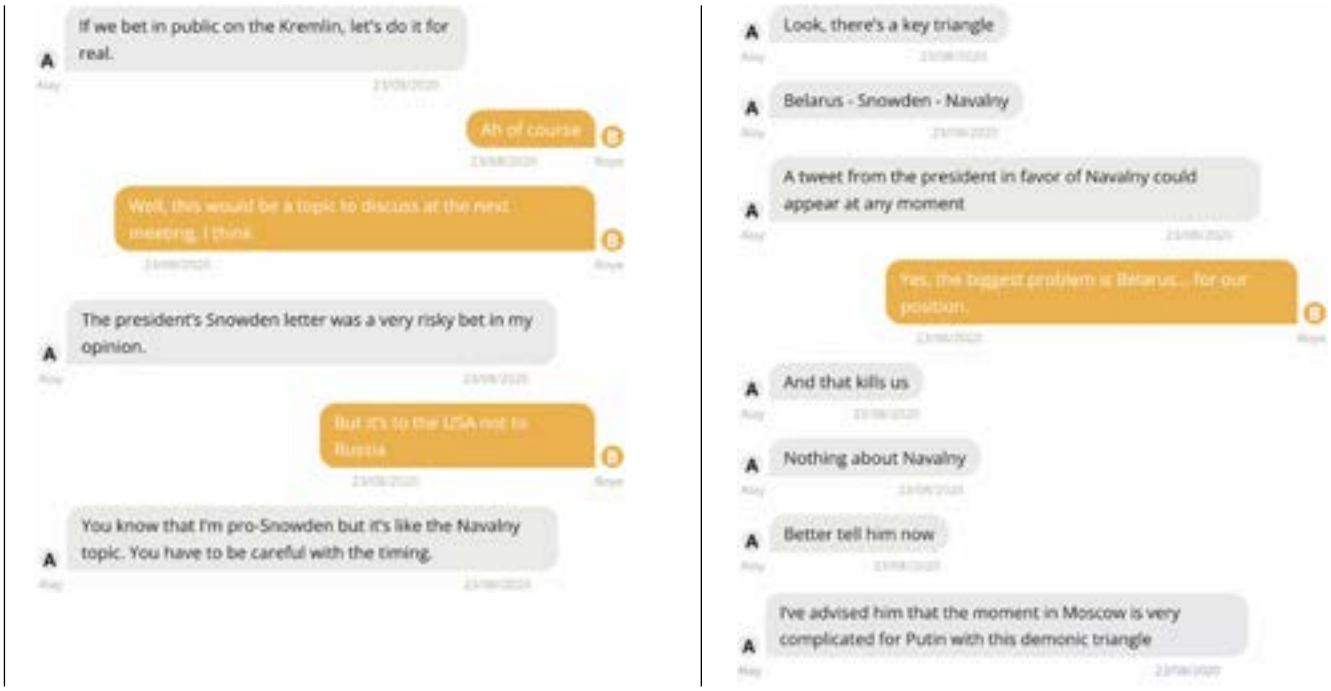



**Josep Lluís Alay**
@josepalay

L'espia soviètica russa Elena Vavilova **@E_VavilovaFoley** també va ser a Barcelona en una data indeterminada.
Després de finalitzar el seu servei per al KGB i SVR, es dedica a escriure novel·les d'espionatge des de Moscou.

5 de agosto de 2021

En conversaciones privadas filtradas a la OCCRP, los Sres. Alay y Boye debaten la posición pública del Sr. Puigdemont frente a Rusia y Snowden. El Sr. Alay también muestra al Sr. Boye una conversación privada con Evgeny Primakov, antiguo político y diplomático, recientemente nombrado jefe de la agencia del Gobierno ruso Rossotrudnichestvo, en la que compara la situación en Cataluña con las «cosas opresivas que se están haciendo a los rusos en Ucrania».[352]




En el último de sus viajes a Moscú, en febrero de 2020, justo meses antes de la filtración de los nombres de los líderes catalanes supuestamente atacados por Pegasus, el Sr. Alay se entrevistó presumiblemente con el Sr. Edward Snowden,[353] que se convirtió en una figura clave en la campaña en los medios de comunicación del referéndum de independencia en octubre de 2017, junto con Julian Assange.

*352/* *OCCRP. 3 de septiembre de 2021. Catalan Separatists Tailored Public Messaging to Avoid Antagonizing Russia: 'You Have to Avoid Navalny For Sure'* https://www.occrp.org/en/investigations/catalan-separatists-tailored-public-messaging-to-avoid-antagonizing-russia-you-have-to-avoid-navalny-for-sure

*353/* *Apparently, Mr Snowden was "first on the agenda" of Mr Alay's visit. OCCRP. Catalan Separatists Tailored Public Messaging to Avoid Antagonizing Russia: 'You Have to Avoid Navalny For Sure'. 3 de septiembre de 2021,* https://www.occrp.org/en/investigations/catalan-separatists-tailored-public-messaging-to-avoid-antagonizing-russia-you-have-to-avoid-navalny-for-sure

*El Confidencial. Emissaries of the Catalan government had been travelling to Moscow up until 2020 to secretly obtain Putin's support. 14 de marzo de 2022,* https://www.elconfidencial.com/espana/2022-03-14/emissaries-catalan-government-travelled-moscow_3390880/

Juntos, los tuits de Snowden y Assange en apoyo a la secesión catalana representaron más de un tercio de todo el tráfico de Twitter con la etiqueta #Catalonia.[354] El Sr. Assange o el Sr. Snowden nunca habían mostrado ningún interés particular por la política española ni por Cataluña antes de 2017. Sin embargo, los dos hombres han sido sospechosos de tener vínculos con los servicios secretos rusos,[355] y han sido decisivos para inclinar la narrativa a favor del nacionalismo catalán inmediatamente antes del referéndum ilegal de octubre de 2017. Hashtagify estableció que el Sr. Snowden, el Sr. Julian Assange, Wikileaks y RT fueron las cuatro cuentas más influyentes de #Catalonia.[356] Assange, por ejemplo, tuiteó 97 veces en catalán, una lengua que no habla, entre septiembre de 2017 y abril de 2019, y el 1 de octubre de 2017 tuiteó 109 veces sobre Cataluña.[357]

*354/* *The Guardian. Disruption games: why are libertarians lining up with autocrats to undermine democracy? 19 de noviembre de 2017, https://www.theguardian.com/technology/2017/nov/19/trump-russia-fake-news-libertarians-autocrats-democracy*

*Political Capital. How How Assange and Snowden led the Russian forces in Catalonia, 17 de mayo de 2019, https://politicalcapital.hu/russian_sharp_power_in_cee/publications.php?article_read=1&article_id=2417*

*355/* *p. ej. , Reuters. La inteligencia rusa manipula a Snowden, dice el ex director de la NSA. 7 de mayo de 2014. https://www.reuters.com/article/oestp-seguridad-eeuu-snowden-idESKBN0DN1BH20140507*

*New York Times. After Arrest of Julian Assange, the Russian Mysteries Remain. 11 de abril de 2019, https://www.nytimes.com/2019/04/11/us/politics/julian-assange-wikileaks-russia.html*

*Al Jazeera. The trouble with Edward Snowden. 18 de diciembre de 2022, https://www.aljazeera.com/opinions/2022/12/18/the-trouble-with-edward-snowden*

*356/* *The Sydney Morning Herald. On Catalan independence, Julian Assange, Edward Snowden emerge as surprise backers. 26 de septiembre de 2017. https://www.smh.com.au/world/on-catalan-independence-julian-assange-edward-snowden-emerge-as-surprise-backers-20170926-gyoqxs.html*

*357/* *El Mundo. Julian Assange: un tuit cada 13 minutos a favor del 'procés'. 12 de abril de 2019, https://www.elmundo.es/papel/historias/2017/12/07/5a27f628ca474121568b4588.html*

El 21 de septiembre de 2017, Snowden compartió el artículo de opinión del Sr. Puigdemont publicado por The Guardian y se refirió a los intentos españoles de impedir el referéndum ilegal como «una violación de los derechos humanos».[358]

*Créditos: El Confidencial, Sr. Alay, visita el periódico ruso Komsomolskaia Pravda en 2019.*[359]

La Guardia Civil española vincula al Sr. Snowden, al Sr. Assange y a la campaña de desinformación del Kremlin sobre Cataluña con Oriol Soler,[360] colaborador del Sr. Puigdemont, y que también fue detenido e investigado, junto con los Sres. Alay, Madi y Vendrell, por su relación con la organización de Tsunami Democràtic.[361] Además, el Sr. Gonzalo Boye también visitó al Sr. Snowden en 2019 y manifestó públicamente que Pegasus se estaba utilizando para espiar a abogados, solo unos meses antes de que estallara el escándalo en Cataluña.[362] En agosto de 2020, tres presuntas víctimas catalanas, los Sres. Puigdemont, Alay y Ponsati firmaron una petición al Sr. Donald Trump solicitando el indulto del Sr. Snowden.[363]

Finalmente, el Sr. Snowden ha sido preseleccionado por partidos secesionistas catalanes para testificar en la comisión Pegasus del Parlament.[364]

*358/* *Edward Snowden. @Snowden. Twitter. 21 de septiembre de 2017, https://twitter.com/Snowden/status/910882660960088065?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E910891664490860545%7Ctwgr%5E61d1601bfaca49b2e526c4e8b925b03a455a26c4%7Ctwcon%5Es4_&ref_url=https%3A%2F%2Fwww.elpuntavui.cat%2Fpolitica%2Farticle%2F-%2F1244594-edward-snowden-denuncia-la-repressio-espanyola-a-catalunya.html*

359/ *El Confidencial, El n.º 2 de Puigdemont visitó un diario del Kremlin en 2019 y se fotografió con un retrato de Putin. 3 de marzo de 2022, https://www.elconfidencial.com/espana/2022-03-03/ucrania-rusia-putin-puigdemont-alay-kremlin-diario_3385059/ Durante mucho tiempo, el Sr. Alay utilizó esta imagen en su perfil de Twitter.*

360/ *Catalan News. Businesspeople related to independence push detained. 28 de octubre de 2020, https://www.catalannews.com/politics/item/businesspeople-related-to-independence-push-detained*

361/ *20 minutos. Quién es Oriol Soler, detenido en una investigación del «procés» y de Tsunami Democràtic, 28 de octubre de 2020, https://www.20minutos.es/noticia/4434070/0/quien-es-oriol-soler-detenido-investigacion-proces-tsunami-democratic/*

362/ *Edward Snowden, @Snowden. Twitter. 9 de noviembre de 2019, https://twitter.com/Snowden/status/1193227686358999045?s=20 and https://twitter.com/Snowden/status/1193232647427895297?s=20*

*Gonzalo Boye. @boye_g. Twitter. 9 de noviembre de 2019, https://twitter.com/boye_g/status/1193228293316730880?s=20*

363/ *Catalan News. Businesspeople related to independence push detained. 28 de octubre de 2020, https://www.catalannews.com/politics/item/businesspeople-related-to-independence-push-detained*

364/ *Parlament de Catalunya, Departament de Comunicació. Compareixences aprovades per la 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, 20 de enero de 2023, https://www.parlament.cat/web/actualitat/noticies/index.html?p_format=D&p_id=270482494*

**Edward Snowden**
@Snowden

The Spanish crackdown on inconvenient speech, politics, and assembly in **#Catalonia** is a violation of human rights.

theguardian.com
**Spain's attempt to block Catalonia's referendum is a violation of our basic right...**

**Gonzalo Boye**
@boye_g

Excelente reunión con **@Snowden @benwizner @WolfgangKaleck** y el resto del equipo jurídico encargado de su defensa... porque no todo es Derecho

5:31 PM · 17 de febrero de 2020

Aunque todos estos vínculos puedan ser fruto del azar, es difícil comprender por qué Citizen Lab los ignoró completamente al establecer hipótesis de la autoría del espionaje y su posible legalidad. Varias partes interesadas internacionales podrían tener un claro interés en vigilar a estos políticos y activistas, ya que podrían contribuir a una operación de desestabilización que podría tener consecuencias de gran alcance para Europa. Los servicios secretos rusos pueden estar interesados en aumentar el número de víctimas en la denuncia como medio para desacreditar a España y a los gobiernos occidentales en general. El funcionamiento de la injerencia política en Europa es bien conocido y ha afectado a otros países como el Reino Unido y Francia.[365] Esta omisión parece más inusual dada la gran preocupación que el Sr. Deibert expresó públicamente en relación con la guerra digital rusa hasta 2017 (ver los tweets a continuación) .[366]

*365/* *France TV. La Fabrique du Mensonge Au cœur de la propagande russe. 11 de diciembre de 2022, https://www.france.tv/france-5/la-fabrique-du-mensonge/la-fabrique-du-mensonge-saison-3/4367680-au-coeur-de-la-propagande-russe.*

*Carnegie Europe. Russia's Long-Term Campaign of Disinformation in Europe. 19 de marzo de 2020, https://carnegieeurope.eu/strategiceurope/81322*

*366/* *Since 2017, Citizen Lab does not seem to have investigated Russian hacking and phishing operations —and focused only on Kremlin's online censorship—.Citizen Lab. Search Result for: Russia https://citizenlab.ca/?s=Russia*

**Edward Snowden** @snowden · 9 de nov, 2019

Government claim they hack people to prevent "crime and terrorism", but **@NYTimes** finds even democraticies are now routinely hacking "human rights activists, journalists, religious leaders and disidents".

An important story, and perhaps a final warning:

nytimes.com
**Spyware Maker NSO Promises Reform but Keeps Snooping (Published...**

**Gonzalo Boye** @boye_g · 9 de nov, 2019

Replying to **@Snowden** and **@nytimes**

And lawyers!!!

**Edward Snowden**
@Snowden

Replying to **@boye_g** and **@nytimes**

Definitely, definitely lawyers.

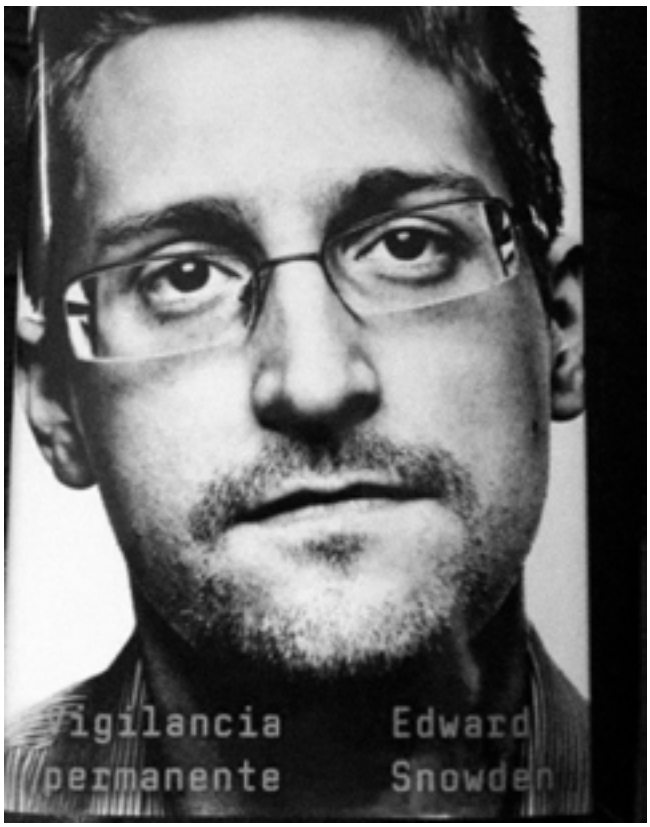
9 de noviembre de 2019

**Josep Lluís Alay**
@josepalay

Vigilància permanent de **@Snowden.**
Una descripció acurada de la Catalunya d'avui sota la vigilància pemanent legal i il·legal dels cossos policials espanyols.

**Gonzalo Boye**
@boye_g

"Vigilancia permanente" un libro imprescindible escrito por **@Snowden**




Sep 23, 2019

**Edward Snowden** @Snowden · 21 de oct, 2019

Everyone knows **@boye_g** recognizes the Spanish police's "search" for what it is: political repression. It should alarm us that even in democracies lawyers, publishers, and ordinary people are facing retaliation for work involving political principles.
ecchr.eu/nc/en/press-re...

**Gonzalo Boye**
@boye_g

Replying to **@Snowden**

Thanks Edward for your support

9 de noviembre de 2019

**profdeibert**
@RonDeibert

A segment of Russia's influence operations have pivoted to Spanish speaking audiences, amplifying consipracies about bio-labs and nuclear contamination

RT and Sputnik in Spanish boosted by Russian embassy tweets and suspicious accounts by **@DFRLab**

17 de marzo

**profdeibert**
@RonDeibert

Russia hackers had targets worldwide, beyond US election apnews.com/3bca5267d45445... Overlap w Tainmted Leaks report: citizenlab.ca/2017/05/tainte...

07 de noviembre de 2017

**profdeibert**
@RonDeibert

See for example our piece "Cyclones in Cyberspace" (2012) about Russia-Georgia conflict journals.sagepub.com/doi/abs10.117...

15 de marzo de 2017

**profdeibert**
@RonDeibert

Russia's Winning the Electronic War foreignpolicy.com/2015/10/21/rus...

22 de octubre de 2015

**profdeibert**
@RonDeibert

How Russia Targets U.S. Military Vets with trolls, fake news politi.co/2rhgLNx via **@politicomag**

12 de junio de 2017

**profdeibert**
@RonDeibert

Russia's Hybrid Warriors Got the White House. Now They're Coming for America's Town Halls. foreignpolicy.com/2017/09/26/rus...

03 de octubre de 2017

**profdeibert**
@RonDeibert

Germany says Russia probably behind cyber attack on Bundestag reut.rs/1TaAPUy via **@Reuters**

13 de mayo de 2016

**profdeibert**
@RonDeibert

Special Report: HP Enterprise let Russia scrutinize cyberdefense system used by Pentagon reut.rs/2x9RdA0

22 de octubre de 2015

**profdeibert**
@RonDeibert

A reconstruction of Russia's Twitter disinformation, influence op in the last hours of 2016 elections thebea.st/2hRDdWO?source... via **@thedailybeast**

08 de noviembre de 2017

**profdeibert**
@RonDeibert

Putin brings China's Great Firewall to Russia in cybersecurity pact theguardian.com/world/2016/nov...

29 de noviembre de 2016

**profdeibert**
@RonDeibert

Once a Defender of Internet Freedom, Putin Is Now Bringing China's Great Firewall to Russia huffingtonpost.com/andrei-soldato... via **@theworldpost**

04 de mayo de 2016

Una hipótesis no confirmada pero verosímil, es que la excelente relación que el Sr. Snowden mantiene tanto con el Sr. Boye como con el Sr. Deibert pudiese haber pesado en la decisión de Citizen Lab de considerar al Sr. Boye, al Sr. Alay y a otros participantes en el informe relacionados con Rusia y Tsunami Democràtic como «víctimas» y no como sospechosos de acciones penales contra España.[367] Su confianza y admiración mutua se ha manifestado constantemente desde 2013, cuando el antiguo agente de la NSA concedió una parte importante de los documentos filtrados al Sr. Deibert, que impulsaron el perfil internacional de Citizen Lab y ayudaron a trabajar contra la vigilancia digital patrocinada por el Estado.[368]

El Sr. Deibert ha entrevistado al Sr. Snowden, organizó un Q&A con su abogado e incluso ha invitado al Sr. Snowden a solicitar una *fellowship* Citizen Lab.[369] el Sr. Snowden aparece en «Black Code», un documental sobre el trabajo del Sr. Deibert;[370] ha denunciado públicamente el Grupo NSO y difundido las pruebas de Citizen Lab y Amnesty Tech contra la empresa israelí de programas espía.[371] También ha elogiado la labor del Sr. Deibert:

## «Nadie ha hecho más que Ron Deibert y su laboratorio para exponer a los enemigos de Internet».[372]

**Edward Snowden**
*Cita en la portada del libro "Reset: Reclaiming the internet for civil society" del Sr. Deibert*

*367/* *Los Sres. Snowden, Deibert y Boye tienen un conocimiento personal común: periodista de alto nivel Glenn Greenwald. Los cuatro han defendido públicamente a Julian Assange. No obstante, el Sr. Greenwald ha borrado sus intercambios en Twitter con el Sr. Boye. Véase José Javier Olivas. @josejolivas. Twitter.* https://twitter.com/josejolivas/status/1530117887758942208?s=20&t=YXO9-_0mUdYieOfrq8HDJw

https://twitter.com/josejolivas/status/1530117902510301186?s=20&t=YXO9-_0mUdYieOfrq8HDJw

https://twitter.com/josejolivas/status/1530117914698948609?s=20&t=YXO9-_0mUdYieOfrq8HDJw

https://twitter.com/josejolivas/status/1530117939638194182?s=20&t=YXO9-_0mUdYieOfrq8HDJw

368/
*See Mr Deibert's testimony. CBC. I received a chunk of the Snowden disclosures — and what I learned blew my mind. 9 de noviembre de 2020,*
*https://www.youtube.com/watch?v=eWqnmGqpPZY*

369/
*Deibert, R. (2016). My conversations with Edward Snowden. 3 de abril de 2016.*
*https://deibert.citizenlab.ca/2016/04/chatting-with-snowden/*

*Access Now. Fireside Chat: Ron Deibert, Edward Snowden & Amie Stepanovich - The Hub. Youtube. 1 de abril de 2016,*
*https://www.youtube.com/watch?v=yGDqXokPGiE*

*University of Toronto. Snowden lawyer discusses need for Citizen Lab with director Ron Deibert. 4 de febrero de 2016,*
*https://politics.utoronto.ca/2016/02/snowden-lawyer-discusses-need-for-citizen-lab-with-director-ron-deibert/*

370/
*IMDB. Black Code. 2016.*
*https://m.imdb.com/title/tt5937964/*

371/
*CTECH. Edward Snowden Slams Israeli Spyware Firm. 7 de noviembre de 2018,*
*https://www.calcalistech.com/ctech/articles/0,7340,L-3749337,00.html*

*The Wire. Youtube. Your Smartphone Is Worse Than A Spy in Your Pocket: Edward Snowden. 22 de julio de 2021,*
*https://www.youtube.com/watch?v=quj2NG34834*

*Mr Snowden also seems to be a personal acquaintance of Mr Guarnieri, the tech lead at Amnesty Tech and former Citizen Lab Fellow. See for instance the event at Studentersamfundet i Trondhjem. Meet Snowden. Youtube. 11 de marzo de 2018,*
*https://www.youtube.com/watch?v=nQ83xLdOtCQ*

372/
*Deibert, R. (2020). Reset: Reclaiming the Internet for Civil Society. The CBC Lectures. House of Anasi Press.*
*https://houseofanansi.com/products/reset*

**Edward Snowden**
@Snowden

Reporters writing on te Apple-NSO stry sould understand this lawsuit would not be *possible* without years-long investigations of @citizenlab, who are close to single-handedly responsible for uncovering the bulk of what we know about the NSO group's darkest deeds.

> **John Scott-Railt...** Jun 28
> BREAKING NOW: @Apple just filed a major lawsuit against NSO Group.
>
> Apple also notifying some recent targets...
> Show this thread

23 de noviembre de 2021

**Edward Snowden**
@Snowden

Huge: @citizenlab catches ISPs invisibly redirecting download requests for popular programs, injecting them with government spyware. Unencrypted web traffic is now provably a critical, in-the-wild vulnerability. 20-30% of top internet sites affected.

citizenlab.ca
**BAD TRAFFIC: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey...**

15:03 · 09 de marzo de 2018

**Edward Snowden** @Snowden · 21 de jul, 2021

Replying to **@rj_gallagher**

You do know Amnesty & Citizenlab actually examined phones whose numbers were on the list and found forensic evidence of Pegasus, right? Pretty irresponsible to amplify an obviously false statement.

**Edward Snowden** @Snowden · 21 de jul, 2021

Replying to **@Snowden and @rj_gallagher**

Every story makes it clear that the 50k figure refers to a superset of people who were entered into a system (such as for HLR lookups), but did not necessarily have exploits launched against them. Hulio is trying to muddy the waters without commenting on confirmed infections.

**Edward Snowden**
@Snowden

Here's the question: if the list of numbers was delivered from Mars, so long as forensically examining many of the phones bearing those numbers were in fact infected by Pegasus, who should we look to for an explanation?

The answer is not Martians, but NSO.

3:59 · 22 de diciembre de 2017

**Edward Snowden**
@Snowden

Haaretz confirms reports by **@Citizenlab** showing Saudi Arabia's purge of regime opponents was fueled by the **#NSO** group, an out of control Israeli hacking company. Before Khashoggi's murder, three of his contacts were targeted by SA using NSO's burglary kit.

haaretz.com
**Israeli NSO negotiated with Saudis advanced cyberattack capabilities sale, Haaretz reveals...**

El Sr. Snowden parece reconocer que a veces las listas de presuntas víctimas de Pegasus se han filtrado a Citizen Lab:

«Esta es la pregunta: si la lista de números se entregó desde Marte, mientras el examen forense de muchos de los teléfonos que llevan dichos números concluya que estaban realmente infectado por Pegasus, ¿a quién deberíamos pedir una explicación? La respuesta no es a los marcianos, sino a NSO».[373]

Extrañamente, en un vídeo publicado por Anonymous en 2021, el Sr. Snowden recomienda a la gente que se ponga en contacto con Citizen Lab cuando crea que está siendo espiado, pero pretende no conocer al Sr. Deibert, solo unos meses después de que escribiera sus comentarios elogiándolo.[374]

«...con ese enlace, pero debéis mandarlo a un grupo como Citizen Lab. Está dirigido por un tipo llamado Ronald Deibert, creo, tendréis que comprobarlo, creo que acaba de publicar un libro sobre todo esto. Pero son los líderes mundiales, en mi opinión, básicamente».

373/ *Edward Snowden. @snowden. 21 de julio de 2021, https://twitter.com/Snowden/status/1417885711517298694?s=20&t=6A-1NbPb0eY26SYm9Mk_eQ*

374/ *Anonymous Oficial. Nobody Knows About This "Prepare Yourself". Youtube. 24 de febrero de 2021, https://www.youtube.com/watch?v=d40oHhECx_I*

Si la relación del Sr. Snowden con los Sres. Deibert y Boye tiene algo que ver con la investigación de CatalanGate, sigue siendo una conjetura, pero lo que parece confirmado es que muchas de las presuntas víctimas en esta investigación han intentado ocultar su relación con Rusia. Los contactos entre los agentes del Kremlin y el nacionalismo catalán parecen avergonzar a parte de este movimiento y, en particular, algunos de los participantes en la investigación de CatalanGate. Por ejemplo, Josep Rius afirmó que los intentos de vincular al Sr. Puigdemont con Rusia eran *fake news* durante un debate parlamentario celebrado el 7 de abril de 2020,[375] y la Sra. Riba afirmó que «puedo confirmar que la Generalitat de Cataluña nunca tuvo contacto con Rusia, nunca, y mi partido ahora está en la Generalitat de Cataluña... nunca, nunca tendremos contacto con Rusia desde la Generalitat de Cataluña» en una audiencia pública en el Consejo de Europa, el 12 de diciembre de 2022.[376] Dos días después de la declaración de la Sra. Riba, una red de televisión francesa emitió un documental en el que Victor Terradellas, asistente del Sr. Puigdemont, confirmó lo que ya había confirmado en el juzgado:[377] que los emisarios de Rusia se habían reunido con la Generalitat en la Casa dels Canonges, residencia oficial del Presidente de la Generalitat el 26 de octubre de 2017. Su debate giró en torno a la independencia de Cataluña y, durante dicha reunión, los emisarios rusos afirmaron que, una vez declarada la independencia, podían proporcionar ayuda financiera y militar.[378] Al menos, Citizen Lab podría haber considerado esta conocida relación como una posible limitación o salvedad en su informe y haber adoptado algunas medidas de precaución para evitar posibles injerencias de Rusia o de quienes colaboran con ella.

375/ *Crónica Global. El Parlament rechaza condenar los "contactos" de Puigdemont y su entorno en Rusia. 7 de abril de 2022, https://cronicaglobal.elespanol.com/politica/parlament-evita-condenar-contactos-puigdemont-entorno-rusia_637368_102.html*

376/ *Pace public hearing, 1:11:00. https://www.youtube.com/watch?v=zZft_l0cWJs*

377/ *El País. Un investigado declara que un emisario del Kremlin ofreció en 2017 a Puigdemont una videollamada con Putin. 11 de mayo de 2022, https://elpais.com/espana/catalunya/2022-05-11/un-investigado-declara-que-puigdemont-se-reunio-con-un-exdiplomatico-ruso-en-pleno-proces.html*

378/ *The Objective. Un asesor de Puigdemont admite por primera vez que Rusia les ofreció 10.000 soldados. 15 de diciembre de 2022, https://theobjective.com/espana/2022-12-15/asesor-puigdemont-rusia/*

# 13

# Reacción inusual de la Universidad de Toronto

Se enviaron al menos tres solicitudes diferentes para abrir una investigación en profundidad en la Munk School, Universidad de Toronto, sobre el informe «CatalanGate; Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru» publicado el 18 de abril de 2022:

→ *Una carta firmada por 16 profesores de diversas instituciones de investigación (entre ellos: Universitat de Barcelona, Real Instituto Elcano, Leiden University, Queen Mary University, CIDE, UNED, CSIC, Universidad de Granada, IE Business School) el 20 de mayo de 2022, junto con un documento de 20 páginas que resume una serie de cuestiones éticas y metodológicas detectadas en el informe "CatalanGate".* [379]

→ *El 5 de julio de 2022 se envió una carta firmada por más de 100 profesores e intelectuales independientes de diversas instituciones (como la Yale University, la Universidad de Sevilla, la Harvard Medical School, la University of Northumbria, la Universitat Autònoma de Barcelona, la Universidad Carlos III, la Universitat Pompeu Fabra, la Beijing Foreign Studies University, etc.).*[380]

→ *El eurodiputado Jordi Cañas envió una carta el 12 de julio de 2022.*

Estas peticiones estaban motivadas por los graves problemas metodológicos y éticos de investigación detectados en el informe, por los testimonios públicos de muchos de los participantes y por la declaración formal que el director de Citizen Lab, Ronald Deibert, hizo pública el 13 de mayo de 2022. La intervención del Sr. Deibert responde a una lista de preguntas presentadas por un grupo de eurodiputados al Parlamento Europeo del Grupo Renew al presidente de la Universidad de Toronto, Meric Gertler, el 11 de mayo de 2022. Las respuestas del Sr. Deibert incrementaron las sospechas de mala práctica, debido a las contradicciones con los testimonios de los participantes, las omisiones deliberadas y la determinación de evitar compartir cualquier información pertinente que pudiera ser utilizada por otros investigadores para validar o reproducir algunos de los análisis que habían dado lugar a conclusiones y acusaciones muy sólidas contra una empresa privada y el Gobierno de España

379/ *Carta a la Universidad de Toronto de 20 de mayo de 2022, https://paginadelforodeprofesores.files.wordpress.com/2022/05/letter-to-uoft-recommending-independent-investigation-citizen*

380/ *Carta a la Universidad de Toronto de 2 de julio de 2022, https://paginadelforodeprofesores.files.wordpress.com/2022/07/letter-to-university-of-toronto-by-foro-de-profesores-5-july-2022-re-catalangate-report.pdf*

La solicitud de apertura de la investigación incluía un documento de observaciones con 22 páginas de pruebas, y en él se pedían respuestas en relación con una multitud de cuestiones compatibles con casos de mala conducta en la investigación,[381] tal como se recoge en la sección 4 del Framework to Address Allegations of Research Misconduct of the University of Toronto (Marco para la resolución de la mala conducta en la investigación de la Universidad de Toronto),[382] entre ellas la posible fabricación de datos, la mala conducta financiera, el no proporcionar información o material relevante al comité de ética de investigación de la Universidad, declaraciones falsas o engañosas contrarias a la buena fe, el no incluir colaboradores que participaron en los análisis forenses del informe, tergiversación deliberada de las conclusiones, etc. Esta carta, aunque iba dirigida a Lorraine Ferris, vicepresidenta asociada encargada de la supervisión y cumplimiento en la investigación en la Universidad de Toronto, fue remitida también al presidente de la Universidad, al director de la Escuela Munk, al director de auditoría interna, al director del Citizen Lab, al presidente del Consejo de Investigación sobre Ciencias Sociales y Humanidades, y a varios eurodiputados del Parlamento Europeo.

La Sra. Lorraine Ferris respondió desestimando la petición el 31 de mayo de 2022 e ignorando las pruebas aportadas. La primera parte de la carta intentó aclarar varios de los aspectos de la petición y algunas de las acusaciones de que aparentemente había malinterpretado en varios correos electrónicos — el 1 de junio, el 22 de junio y el 14 de julio de 2022 — y le recordaba que la solicitud de una investigación interna se ajustaba a los Principios de Buena Gobernanza[383] de la Universidad de Toronto, su política de integridad en la investigación,[384] y el informe de 2010 del Grupo de Expertos sobre Integridad en la Investigación[385], así como a las expectativas académicas básicas en materia de transparencia y rendición de cuentas públicas. Además, en el correo electrónico enviado el 14 de julio de 2022 se incluyeron nuevas alegaciones de posibles irregularidades en la investigación. Sin embargo, todas las respuestas dadas por la Universidad de Toronto fueron elusivas y el último mensaje recibido de la Sra. Ferris, el 18 de julio de 2022, fue simplemente una respuesta idéntica a la que envió para rechazar las otras dos cartas que habían solicitado una investigación independiente, una de un grupo de más de 100 profesores de muchas universidades diferentes y otra del eurodiputado Jordi Cañas. El último mensaje enviado el 19 de julio de 2022 se dirigió exclusivamente al Sr. Peter Loewen, director de la Munk School of Global Affairs and Public Policy, pero nunca respondió.

El autor de esta revisión también se puso en contacto con los miembros del Consejo de Ética de la Investigación de la Universidad de Toronto sobre la participación del Sr. Elies Campo en la investigación, la revelación de posibles conflictos de intereses, la divulgación de cuestiones éticas potencialmente problemáticas en relación con la investigación específica en Cataluña y la financiación de esta investigación. Sin embargo, la respuesta de Margaret Pichora-Fuller el 29 de abril de 2022 fue muy breve, ambigua e ignoró la mayoría de las preguntas. La solicitud de

seguimiento dirigida a la Sra. Pichora-Fuller ese mismo día no recibió respuesta. Probablemente, no se solicitaron ni se concedieron autorizaciones específicas en relación con la investigación en Cataluña, y el Consejo de Ética no fue informado de que los partidos políticos estaban llevando a cabo análisis forenses y seleccionando casos para el informe. Esto parece como si el Consejo de Ética de la Universidad concediera a Citizen Lab vía libre en el proyecto Pegasus, y Citizen Lab hubiera interpretado que podía actuar de manera similar en las democracias y en los países autoritarios, suponiendo la ausencia de Estado de Derecho y la ilegalidad del control policial.

Conceder una licencia general de este tipo para llevar a cabo investigaciones muy sensibles (sin necesidad de una ulterior comprobación de los agentes de la ética de la investigación) y bloquear cualquier intento de poner en marcha una iniciativa independiente es extremadamente problemático. La Universidad de Toronto puede estar creando involuntariamente incentivos para un comportamiento temerario y no académico. Los conflictos de interés observados, tanto los materiales como los políticos, sumados a una conducta con graves carencias de transparencia y responsabilidad puede ser interpretada como contraria al ethos de la investigación académica. No está claro si este caso es representativo de una política de ética de investigación sorprendentemente laxa en la Munk School y la Universidad de Toronto, o si se trata simplemente de una simple excepción que ilustra la existencia de normas y expectativas diferenciadas para cumplir las normas éticas habituales en materia de investigación en ciencias sociales en estas instituciones canadienses.

Dada la falta de colaboración y de explicaciones creíbles por parte de la Oficina de Vigilancia y Cumplimiento de la Investigación y del Consejo de Ética de la Investigación, se contactó con el *Ombudsman* de la Universidad de Toronto, Bruce Kidd, el 22 de julio de 2022, y se le pidió que interviniera formalmente en el asunto y convenciera a la Universidad de Toronto y a la Munk School para que iniciaran una investigación sobre el tema.

*381/* *Olivas Osuna, J.J. (2022). Methodological and ethical issues in Citizen Lab's spyware investigation in Catalonia, document publicly available on ResearchGate: https://www.researchgate.net/publication/361140330_Methodological_and_ethical_issues_in_Citizen_Lab's_spyware_investigation_in_Catalonia*

*382/* *Framework to Address Allegations of Research Misconduct of the University of Toronto (2013) https://research.utoronto.ca/media/48/download*

*383/* *El preámbulo de los principios de buena gobernanza de la Universidad de Toronto hace referencia a: «... la necesidad de ser considerada responsable, a través de la transparencia, ante todas las partes interesadas en la Universidad...» Universidad de Toronto. Consejo de Gobierno. Principios de buena gobernanza (2010). https://governingcouncil.utoronto.ca/system/files/import-files/principles7288.pdf*

384/ *Página de Integridad de la Investigación. La Universidad de Toronto afirma: «U of T se esfuerza por mantener los niveles más elevados de integridad de la investigación y responderá a las acusaciones de mala conducta en la investigación de conformidad con el Marco para la resolución de la mala conducta en la investigación». Universidad de Toronto. https://research.utoronto.ca/research-integrity/research-integrity*

385/ *Expert Panel on Research Integrity (2010). Honesty, Accountability and Trust: Fostering Research Integrity in Canada. Council of Canadian Academies https://cca-reports.ca/wp-content/uploads/2018/10/ri_report.pdf*

Sin embargo, el Sr. Bruce Kid rechazó la solicitud alegando que alguien de fuera de la Universidad no podía entrar en el ámbito de su jurisprudencia, y también manifestó que, si alguien entrara en el ámbito de su jurisprudencia, sería redirigido a la oficina de vigilancia y cumplimiento en la investigación antes mencionada:

«El mandato del *Ombudsman* de la Universidad me impide investigar una reclamación presentada por alguien que no es competencia del Consejo de Gobierno de la Universidad, así como las reclamaciones que no son de nuestra jurisdicción. Tenga en cuenta que, si un miembro de la comunidad de la Universidad de Toronto que estaba bajo nuestra jurisdicción tuviera que ponerse en contacto con nosotros con preocupaciones similares sobre las actividades del Citizen Lab, redirigiríamos su denuncia a la oficina de vigilancia de la investigación de cumplimiento».[386]

Además, el 22 de julio de 2022 se completó una solicitud de la Ley de Libertad de Información y Protección de la Privacidad (FIPPA) (solicitud n.º #22-0052).[387] El 22 de agosto de 2022, Rafael Eskenazi, Director de FIPPA, reconoció que se habían localizado registros que respondían a la solicitud, pero que, dado que los registros podían afectar a los intereses de terceros, tuvieron que realizar una consulta.

El 21 de septiembre de 2022, el Sr. Eskenazi cumplió parcialmente la solicitud formal de transparencia. La solicitud incluía la publicación de 6 tipos de datos:

A → *Ingresos u otras fuentes de financiación recibidas por Citizen Lab desde 2017. Incluida la financiación procedente de Munk School/ Universidad de Toronto, así como del importe detallado de la financiación recibida por cualquier otra institución y particular, incluidos los donantes anónimos, la financiación procedente de subvenciones de investigación, la financiación como pago de servicios potenciales por parte de Citizen Lab a terceros, etc. Indique las fechas en que se efectuaron los pagos o asignaciones.*

B → *Cualquier otro tipo de donación significativa, beneficios, compensación material o regalo recibido por el Citizen Lab o miembros de su facultad.*

La Universidad de Toronto publicó una hoja de cálculo que agrupaba los importes recibidos por Citizen Lab y la fecha, pero no incluía los nombres de las organizaciones que lo financiaron. La financiación de Citizen Lab fue de 1.750.135 CAD para el año académico 2019-2020, cuando se inició la investigación en Cataluña, y la financiación obtenida para el curso académico 2021-2022 fue de 3.713.603 CAD (un aumento del 112 %). La información relativa a los nombres de las entidades financiadoras se solicitó desde entonces en varias ocasiones a la Freedom of Information and Protection of Privacy Office sin resultado alguno. Después de varios intercambios y períodos de tiempo teóricamente necesarios para consultar con las partes afectadas, el 30 de enero de 2023, esta oficina anunció que «la información sobre los financiadores/donantes en las partes A y B de su petición ha sido retenida bajo FIPPA s. 18(1)(c) porque compartirla podría suponer un perjuicio razonable de los intereses económicos de la Universidad o para su posición competitiva».[388] La justificación ofrecida está lejos de ser satisfactoria. Encubrir los nombres de todos los particulares y todas las organizaciones que financian un centro de investigación de una universidad pública es extremadamente inusual y puede ser problemático desde un punto de vista legal.

386/ *Email del Sr. Bruce Kidd al Sr. José Javier Olivas Osuna el 2 de agosto de 2022.*

387/ *El 22 de julio de 2022, José Javier Olivas Osuna presentó digitalmente el formulario A de solicitud de libertad de información y protección de la intimidad a la Oficina de Libertad de Información y Protección de la Privacidad.*

388/ *Email de la Sra. Lindsay Mills al Sr José Javier Olivas Osuna el 2 de enero de 2023.*

C

→ *Información sobre fuentes alternativas de financiación declaradas a Munk School/Universidad de Toronto por los miembros de la Facultad y el personal de Citizen Lab (si no puede revelar los nombres de los beneficuiarios o los nombres de las organizaciones que los emplean o disfrutan de sus servicios fuera de la Munk School/UofT, facilite la información anonimizada, por ejemplo, el miembro del personal nº 1 realiza un trabajo remunerado para una empresa de consultoría en materia de seguridad informática, el miembro del personal nº 2 forma parte de y recibe remuneración por su trabajo en el consejo de administración de una ONG internacional, etc). Incluya todas las actividades alternativas conocidas comunicadas a la Munk School/UofT desde 2017 (incluso las que han cesado en el momento de la solicitud de acceso).*

La Universidad de Toronto determinó que cualquier registro sensible a la parte C de la solicitud quedaría excluido de conformidad con la sección 65 (6) de la FIPPA porque la FIPPA no se aplica a los registros recogidos, elaborados, mantenidos o utilizados por la Universidad o en su nombre en relación con asuntos relacionados con el empleo en los que la Universidad tenga interés.

D

→ *Información sobre cualquier contrato de servicios firmado por Citizen Lab con cualquier organización relacionada con el proyecto Pegasus (podría tratarse de contratos relacionados con servicios prestados o recibidos). Incluya también las fechas, la cantidad y los datos para identificar a la organización o a los contratistas individuales implicados.*

E

→ *Actas de las reuniones de Citizen Lab y Munk School en las que se hizo referencia a la investigación sobre Pegasus o Candiru en Cataluña.*

La Universidad de Toronto alegó que no había encontrado ningún registro que respondiera a las partes D y E de la solicitud, lo que parece muy extraño dada la magnitud del proyecto y los contactos evidentes con partidos y organizaciones independientes desde julio de 2020.

F

→ *Copias de los acuerdos y actas de reuniones entre Citizen Lab y Apple, Citizen Lab y WhatsApp/Facebook, Citizen Lab y cualquier empresa de comunicación/relaciones públicas, así como entre Citizen Lab y cualquier organización o empresa política catalana, desde 2017.*

La Universidad de Toronto localizó 124 páginas de registros que respondían a la parte F de la solicitud, pero fue la decisión de la Universidad de publicar solo 9 páginas completas y 3 páginas en parte, de la siguiente manera:

→ *En línea con la sección 65 (8.1) de la FIPPA, y la FIPPA, se han omitido 112 páginas completas de la divulgación porque contienen información de investigación detallada y porque se podría esperar que su divulgación fuese perjudicial para la investigación.*

→ *Se ha retenido una parte de 1 página, de conformidad con la sección 14 (1) (e) de la FIPPA, porque cabe esperar razonablemente que la divulgación ponga en peligro la vida o la seguridad física de un agente de seguridad o de cualquier otra persona, y de conformidad con la sección 20 de la FIPPA, porque cabe esperar que la divulgación suponga una amenaza para la salud y la seguridad.*

→ *Se han retenido porciones de 2 páginas con arreglo a la sección 21 de la FIPPA porque consisten en información personal, cuya divulgación constituiría una invasión injustificada de la intimidad personal.*

## TABLA 4

## SOLICITUD DE LA FIPPA

UNIVERSITY OF TORONTO

FREEDOM OF INFORMATION & PROTECTION OF PRIVACY OFFICE

September 21, 2022

Dr. José Javier Olivas Osuna

**Delivered via E-Mail (J.J.Olivas-Osuna@lse.ac.uk)**

Dear Dr. José Javier Olivas Osuna:

**Re: Request #22-0052 – Access Decision**

Thank you for your request under the *Freedom of Information and Protection of Privacy Act* (FIPPA) for:

***I would like to request the following information regarding the Citizen Lab:***

***a) Income or other sources of funding received by Citizen Lab since 2017. Including the funding from Munk School / University of Toronto as well from the detailed amount of funding received by any other institution and private individual, including anonymous donors, funding from research grants, funding as payment of potential services by Citizen Lab to third parties, etc. Please provide the dates in which payments or allocations where made.***

***b) Any other type of significant donation, perk, material compensation or gift received by the Citizen Lab or its faculty mers (sic)***

***c) Information about alternative sources of funding declared to Munk School/University of Toronto by the faculty members and staff of the Citizen Lab (if you are not able to reveal the names of the recipients or the names of the organisations that employ them or enjoy their services outside Munk School/UofT, please provide the anonymized information, e.g., staff member 1 conducts paid work for an IT security consulting firm, staff member 2 seats and is paid for their work in the board of an international NGO, etc. Please include all known alternative activities reported to the Munk School/UofT since 2017 (even those that have ceased by the time of the access request).***

***d) Information about any services contract signed by the Citizen Lab with any organization related to the Pegasus project (it could be contracts related to services provided or received). Please include also the dates, amount and data to identify the organisation or individual contractors involved.***

McMurrich Building, 12 Queen's Park Crescent West, Room 104, Toronto, ON, M5S 1A8 Canada
Tel: + 1 416 946-7303 or Tel: + 1 416 978-4873 • www.fippa.utoronto.ca

***e) Minutes from the meetings at Citizen Lab and the Munk School in which there were any references to the Pegasus or Candiru spyware investigation in Catalonia.***

***f) Copies of any agreements and meetings' minutes between Citizen Lab and Apple, Citizen Lab and WhatsApp/Facebook, Citizen Lab and any communication/PR company, as well as between Citizen Lab and any Catalan political organisation or firm, since 2017.***

As detailed in my August 22, 2022 letter to you in this matter, the University provided notice to third parties whose interests may be affected by the disclosure of records responsive to your request and sought representations from third parties regarding those records.

In making its decision, the University carefully considered all relevant factors, including previous Orders of the Information and Privacy Commissioner of Ontario (the IPC) and the submissions of the affected third parties.

It is the decision of the University to respond to the parts of your request as follows:

**Parts A and B of your request:**

In response to parts A and B of your request, please find a spreadsheet (attached as Appendix A to this correspondence) detailing the "[i]ncome or other sources of funding received by Citizen Lab since 2017…(part A), which includes "[a]ny other type of significant donation, perk, material compensation or gift received by the Citizen Lab or its faculty mers (sic)" (Part B).

**Part C of your request:**

The University has determined that any responsive records to part C of your request would be excluded pursuant to section 65(6) of FIPPA because FIPPA does not apply to records collected, prepared, maintained or used by, or on behalf of the University in relation to employment-related matters in which the University has an interest.

**Parts D and E of your request:**

Careful searches by the University did not locate any records responsive to parts D and E of your request.

**Part F of your request:**

A careful search by the University located 124 pages of records responsive to part F of your request. It is the decision of the University to release 9 pages in full and 3 pages in part, as follows:

- 112 full pages have been withheld from disclosure because they contain detailed research information the disclosure of which could reasonably be expected to be harmful to research, consistent with FIPPA section 65(8.1) and FIPPA does not apply to these records;

- A portion of 1 page has been withheld, pursuant to FIPPA section 14(1)(e), because disclosure could reasonably be expected to endanger the life or physical safety of a law enforcement officer or any other person, and pursuant to FIPPA section 20, because disclosure could be expected to threaten health and safety; and

- Portions of 2 pages have been withheld pursuant to FIPPA section 21 because they are comprised of personal information, the disclosure of which would constitute an unjustified invasion of personal privacy.

FIPPA section 50(1) allows you to appeal any decision made by the University, within 30 days, by notifying the Information and Privacy Commissioner/Ontario (the IPC). Therefore, you may appeal this decision within thirty days of the date of this letter. The IPC's contact information is as follows:

2 Bloor Street East
Suite 1400
Toronto, Ontario M4W 1A8
Telephone: 416) 326-3333 (Toll Free: 1-800-387-0073)
Email: info@ipc.on.ca

A third party will also have 30 days to appeal the decision to the IPC pursuant to FIPPA s. 28(8)(a) before any records can be disclosed to you pursuant to FIPPA s. 28(8)(b).

If you choose to appeal this decision, you should quote the above file number to the IPC and provide a copy of your original request and this decision letter. You will also be required to provide the IPC with an appeal fee of $25.00.

If you have any questions, please do not hesitate to contact me via email at rafael.eskenazi@utoronto.ca or by telephone at 416-416-427-4963.

Yours truly,

Rafael Eskenazi

Rafael Eskenazi, Director
Freedom of Information and Protection of Privacy Office

## Appendix A

| End Date | Total Funding | | 2017-18 | 2018-19 | 2019-20 | 2020-21 | 2021-22 | 2022-23 |
|---|---|---|---|---|---|---|---|---|
| | USD/other | CAD | | | | | | |
| 31.12.2021 | 1,000,000 | 1,304,917 | | 328,049 | 327,718 | 649,150 | | |
| 31.10.2021 | 1,400,000 | 1,800,680 | 450,170 | 450,170 | 450,170 | | 450,170 | |
| 31.07.2021 | 450,000 | 586,845 | | 191,703 | 195,876 | 199,266 | | |
| 31.11.2021 | 300,000 | 503,790 | | 167,930 | 167,930 | 167,930 | | |
| 31.01.2022 | - | 355,950 | | | 124,300 | 141,250 | 72,924 | |
| 31.12.2022 | 360,000 | 468,540 | | | 156,180 | 156,180 | 156,180 | |
| 31.12.2022 | 350,977 | 487,469 | 104,167 | 227,875 | 41,667 | | | |
| 31.12.2020 | 150,000 | 200,910 | | 200,910 | | | | |
| 31.10.2021 | 1,100,000 | 1,443,310 | | 949,181 | | 494,129 | | |
| 31.05.2022 | 100,000 | 120,420 | | | | | 120,420 | |
| 30.11.2024 | 450,000 | 765,585 | | | | | 255,195 | |
| 30.12.2025 | | 1,521,600 | | | | | 380,400 | |
| 28.02.2025 | 750,000 | 952,650 | | | | | | 317,550 |
| 31.03.2025 | 300,000 | 375,240 | | | | | | |
| - | 850,000 | 954,295 | 40,362 | 41,167 | 41,972 | 42,828 | 47,196 | |
| - | 540,000 | 664,600 | 274,093 | | | | | |
| 30.09.2020 | 290,000 | 381,176 | | 189,515 | 191,661 | | | |
| 30.09.2022 | 290,000 | 367,744 | | | | 191,801 | 175,943 | |
| - | 25,000 | 33,343 | | | 33,343 | | | |
| - | 200,000 | 251,500 | | | | 251,500 | | |
| - | - | 25,000 | | 5,000 | 10,000 | 10,000 | | |
| - | 16,525 | 21,040 | | | | 21,040 | | |
| | | 10,000 | | | | | 10,000 | |
| | | 100,000 | | | | | 100,000 | |
| | | 89,779 | 2,984 | 3,565 | 9,319 | 21,980 | 44,575 | 7,357 |
| 31.12.9999 | | 1,150,000 | | | | | 1,150,000 | |
| 31.12.9999 | | 750,000 | | | | | 750,600 | |
| | **8,922,502** | **15,686,381** | **871,776** | **2,755,065** | **1,750,135** | **2,347,054** | **3,713,603** | **324,907** |

El 9 de noviembre de 2022, la Universidad de Toronto publicó las páginas correspondientes a dos contratos (excluidos los apéndices):

→ *Contrato de 46.900 CAD con BYFACILITY S.L., representado por Axel Gasulla Roglà (administrador único), para el diseño visual, la parte delantera, la trasera y el mantenimiento de una página web. Contrato firmado por Peter Loewen Director de Munk School of Global Affairs and Public Policy y Melanie Woodin (Universidad de Toronto) el 5 de abril de 2022. Cabe suponer que este contrato tenía por objeto desarrollar la página web de infografías para el informe CatalanGate firmado por Domestic Data Streamers. El importe dedicado a un sitio web infográfico es muy inusual en el mundo académico, donde los presupuestos son muy limitados. Cabe señalar que la empresa está establecida en Barcelona.*[389]

→ *Un contrato de 7.500 CAD con Milan Schramek para crear una animación para complementar un informe de Citizen Lab sobre la represión digital transnacional. El contrato se firmó el 7 de diciembre de 2021.*

Entre las 112 páginas retenidas, hay presuntos contratos firmados entre Citizen Lab y organizaciones políticas catalanas, Apple o WhatsApp/Facebook, pero la Universidad no quiere compartir esta información. Es importante señalar que el Sr. Deibert declaró claramente en una carta formal en respuesta a los eurodiputados de Renew que «Citizen Lab nunca se ha visto inducido a encontrar pruebas de una demanda por parte de ninguna de las partes en un litigio, incluida Apple. En ningún caso realizaríamos una investigación bajo encargo».[390] La existencia de tales contratos parece contradecir las afirmaciones del Sr. Deibert y podría entrañar un conflicto de intereses económicos no divulgados, lo que podría suponer un incumplimiento del marco de integridad de la investigación de la Universidad de Toronto.

*389/* *Sitio web supuestamente encargado por Citizen Lab:* https://catalonia.citizenlab.ca/

*Alex Gasulla Roglà es el socio fundador de Domestic Data Streamers* https://domesticstreamers.com/

*390/* *Carta de Mr Ronald Deibert a Jordi Cañas, página 6.*

Citizen Lab no debería operar en el mundo académico si no está dispuesto a seguir las convenciones académicas básicas, las normas de responsabilidad y el código deontológico. Si no observan el método científicos y simplemente trabajan en la industria o el activismo político, podrían establecerse como una empresa privada o como ONG y continuar su colaboración con las grandes corporaciones tecnológicas y los partidos políticos. Alternativamente, podrían constituirse públicamente como rama consultora de la Universidad y especificar sus fuentes de financiación, así como los intereses económicos y políticos que sustentan su investigación. Presentar como parte académica una investigación que no sigue las normas académicas mínimas es una práctica engañosa.

La indiferencia mostrada por la Sra. Ferris y los otros dirigentes de la Universidad de Toronto que fueron copiados en varios de los intercambios de mensajes y, por tanto, fueron conscientes de las graves alegaciones y de las justificaciones muy insuficientes para no oponerse a las alegaciones del asunto, es muy problemática. Citizen Lab es muy influyente y ha contribuido a llamar la atención de los medios y a aumentar la financiación de la Munk School y la Universidad de Toronto. Sin embargo, si confiaban en que Citizen Lab actuaba respetando su política de integridad de la investigación, ¿por qué actuar de forma tan poco transparente, proporcionando respuestas tardías y ambiguas e ignorando evidencias bien documentadas que apunten a una probable mala conducta en la investigación? Incluso cuando se han puesto de manifiesto las acusaciones formuladas en el informe y la campaña de propaganda para desacreditar hiperbólicalmente a España, una democracia europea y un Estado Miembro de la UE, no han mostrado ninguna preocupación o interés aparente en aclarar posibles errores o malentendidos.

# 14

# Las «víctimas» del «espionaje ilegal»

No está claro por qué, al parecer, Citizen Lab no utilizó ningún grupo de control en la investigación ni por qué no se hace referencia a los análisis de dispositivos de personas que no estaban directamente implicadas en movimientos secesionistas. Citizen Lab no reconoció si, entre los 1.400 usuarios de la lista de WhatsApp, había otros ciudadanos españoles además de los cinco políticos y activistas catalanes mencionados (Sres. Torrent, Maragall, Gabriel, Domingo y Miquel) o cómo descartaban la hipótesis de que los españoles no secesionistas también pudieran ser posibles víctimas de ataques con programas espía. Como se ha sugerido anteriormente, es evidente que el trabajo de campo solo pretendía confirmar la hipótesis del espionaje ilegal por parte del Gobierno español sobre políticos y activistas partidarios de la independencia.

Muchos de los participantes en la investigación eran fugitivos o estaban encarcelados o sometidos a juicio en el momento en que se llevó a cabo la investigación de Citizen Lab. Por ejemplo, Anna Gabriel[391], Marta Rovira,[392] Antoni Comín,[393] Meritxel Serret, Clara Ponsati y Carles Puigdemont eran fugitivos con órdenes de detención,[394] Jordi Sànchez y Jordi Cuixart fueron condenados y encarcelados.[395] Artur Mas,[396] David Madi,[397] Xavier Vendrell[398] , Josep Maria Jové[399] y Gonzalo Boye[400] participaron en procesos judiciales acusados de corrupción y otros delitos durante el trabajo de campo de la investigación de CatalanGate. Otros participantes estaban siendo vigilados con autorización judicial: Elsa Artadi, Albert Batet, David Bonagí, Marc Solsona, Carles Riera, Sergi Miquel, Jordi Baylina, Pau Escrich, Xavier Vives, Marcel Mauri, Elisenda Paluzie, Jordi Bosch, Joan Matamala y Josep Lluis Allay, el Sr. Xavier Vendrell y el Sr. Pere Aragonès.[401] Otras presuntas víctimas también se enfrentaron a investigaciones policiales relacionadas con presuntas actividades ilegales, como Laura Borras, David Fernández, Arià Bayé, Ferran Bel, Joan Ramon Casals y Joaquim Torra (véase el cuadro de víctimas en el anexo).

*391/* *LaVanguardia. La orden de detener a Anna Gabriel tendrá efectos en España e internacionales. 22 de febrero de 2018, https://www.lavanguardia.com/politica/20180222/44970315359/anna-gabriel-orden-detencion-efectos-internacionales-suiza.html*

*392/* *Crónica Global. La Fiscalía pide una orden de actividad y captura internacional contra Marta Rovira, 23 de marzo de 2018, https://cronicaglobal.elespanol.com/politica/fiscalia-orden-busca-captura-marta-rovira_129551_102.html*

*393/* *CoSalud.es. Orden internacional de detención para Antoni Comín, 3 de noviembre de 2017, https://www.consalud.es/autonomias/cataluna/orden-internacional-de-detencion-para-antoni-comin_43656_102.html*

*394/* *LaVanguardia. La juez Lamela emite la Orden Internacional de Busca, Captura y Prisión de Puigdemont. 3 de noviembre de 2017, https://www.lavanguardia.com/politica/20171103/432558010022/juez-orden-detencion-puigdemont.html*

*El País. Estos son los siete Líderes del «procés» huidos de España, 19 de julio de 2018, https://elpais.com/politica/2018/07/19/actualidad/1532005516_928674.html*

395/

*TV3. Notícies. Jordi Cuixart y Jordi Sànchez, condensados a 9 años de CÁRCEL por sedición. 9 de noviembre de 2021, https://www.ccma.cat/324/jordi-cuixart-y-jordi-sanchez-condenados-a-9-anos-de-carcel-por-sedicion/noticia-es/2955685/*

396/

*ABC. Artur Mas, inhabilitado hasta 2020. 5 de febrero de 2019, https://www.abc.es/espana/catalunya/politica/abci-artur-mas-inhabilitado-hasta-2020-201902051229_noticia.html*

397/

*El Periódico. Una jueza liga el proceso por facturas falsas de David Madí al 'caso 3%'. 20 de mayo de 2021, https://www.elperiodico.com/es/politica/20210520/jueza-david-madi-caso-3-facturas-falsas-11746090*

398/

*El Periódico. Una jueza liga el proceso por facturas de David Madí al «caso 3 %». 20 de mayo de 2021, https://www.elperiodico.com/es/politica/20210621/guardia-civil-vendrell-madi-tsunami-11844090*

399/

*El Confidencial. La Fiscalía pide hasta siete años de prisión a los cargos intermedios de ERC por el 1-O, 17 de febrero de 2023, https://www.elconfidencial.com/espana/2023-02-17/la-fiscalia-pide-hasta-7-anos-de-prision-a-los-cargos-intermedios-de-erc-por-el-1-o_3577710/*

400/

*ElDiario.es. La Audiencia Nacional Confirma el proceso por blanco de Gonzalo Boye, abogado de Puigdemont. 28 de junio de 2021, https://www.eldiario.es/politica/audiencia-nacional-confirma-procesamiento-blanqueo-gonzalo-boye-abogado-puigdemont_1_8081620.html*

401/

*ElMón. Pegasus: la llista dels 18 espiats pel CNI amb aval del jutge, al descobert. 14 de mayo de 2022, https://elmon.cat/politica/pegasus-llista-18-espiats-cni-422781/*

La forma en que una gran parte de las «víctimas» de CatalanGate decidió promover de manera coordinada la puesta en marcha de la plataforma Tsunami Democràtic en Twitter el 2 de septiembre de 2019 — todos ellos citando el mismo mensaje en la misma vista— demuestra cómo actuaron como una red bien organizada.

**Diana Riba i Giner**
@DianaRibaGiner

La repressió està sent dura i sabem que la vulneració de drets civils i polítics no s'aturarà. Però el que està en joc és tan important que nosaltres tampoc ens podem aturar.

Siguem, de nou, un **#TsunamiDemocràtic**

> **Tsunami Democràtic** @tsunami_dem · 02 Sep 2019
> Recuperem la iniciativa!
> Amb la noviolència i la desobediència civil com a eines, avancem-nos a la sentència. Canviem l'estat de les coses:...
> Show this thread

02 de setiembre de 2019

**Quim Torra i Pla**
@QuimTorraiPla

Els drets, si no s'exerceixen, perden sentit. La defensa de la democràcia i dels nostres drets civils, polítics i socials, inclòs el dret d'autodeterminació s'ha de fer cada dia. Hi estem compromesos. Sort i endavant! **#TsunamiDemocràtic**

> **Tsunami Democràtic** @tsunami_dem · 02 Sep 2019
> Recuperem la iniciativa!
> Amb la noviolència i la desobediència civil com a eines, avancem-nos a la sentència. Canviem l'estat de les coses:...
> Show this thread

02 de setiembre de 2019

**Elisenda Paluzie**
@epaluzie

Obrim nou cicle, recuperem la iniciativa, sempre des de la noviolència **#TsunamiDemocràtic #ObjectiuIndependència**

> **Tsunami Democràtic** @tsunami_dem · 02 Sep 2019
> Recuperem la iniciativa!
> Amb la noviolència i la desobediència civil com a eines, avancem-nos a la sentència. Canviem l'estat de les coses:...
> Show this thread

02 de setiembre de 2019

**FreeRomeva**
@FreeRomeva

Tic TAC tic TAC tic

> **Tsunami Democràtic** @tsunami_dem · 02 Sep 2019
> Recuperem la iniciativa!
> Amb la noviolència i la desobediència civil com a eines, avancem-nos a la sentència. Canviem l'estat de les coses:...
> Show this thread

02 de setiembre de 2019

**Toni Comín**
@toni_comin

Que el tsunami ja no s'aturi. Acció i mobilització no violenta per respondre a la repressió i desbordar-la. Ens hi juguem la democràcia i les llibertats. **#TsunamiDemocràtic**

> **Tsunami Democràtic** @tsunami_dem · 02 Sep 2019
> Recuperem la iniciativa!
> Amb la noviolència i la desobediència civil com a eines, avancem-nos a la sentència. Canviem l'estat de les coses:...
> Show this thread

02 de setiembre de 2019

**Ernest Maragall i Mira**
@ernestmaragall

Trenquem el mur de repressió, que l'Estat ha volgut construir, amb un nou **#TsunamiDemocràtic** que tingui l'impuls de la mobilització, l'acció col·lectiva i la defensa de la democràcia i de les llibertats, començant per la dels que pateixen presó o exili.

> **Tsunami Democràtic** @tsunami_dem · 02 Sep 2019
> Recuperem la iniciativa!
> Amb la noviolència i la desobediència civil com a eines, avancem-nos a la sentència. Canviem l'estat de les coses:...
> Show this thread

02 de setiembre de 2019

**ANCBrussel·les**
@ANCBru

Our rights are at stake. We are going to defend them by means of non-violent civil disobedience. Since “Freedom is not something that anybody can be given, freedom is something people take, and people are as free as they want to be”. James Baldwin

> **Tsunami Democràtic** @tsunami_dem · 02 Sep 2019
> Recuperem la iniciativa!
> Amb la noviolència i la desobediència civil com a eines, avancem-nos a la sentència. Canviem l'estat de les coses:...
> Show this thread

02 de setiembre de 2019

**Marta Rovira Vergés**
@martarovira

Tal com vam sortir a defensar les urnes i el dret a vot, sortirem a defensar la democràcia i exercir els drets i llibertats tantes vegades com faci falta. Fer un referèndum no es cap delicte. Defensar la independència, tampoc. **#TsunamiDemocràtic**

> **Tsunami Democràtic** @tsunami_dem · 02 Sep 2019
> Recuperem la iniciativa!
> Amb la noviolència i la desobediència civil com a eines, avancem-nos a la sentència. Canviem l'estat de les coses:...
> Show this thread

02 de setiembre de 2019

**David Bonhevi**
@davidbonhevi

Votar mai no ha de ser un delicte, responem tots junts a una possible sentència injusta!!!

> **Tsunami Democràtic** @tsunami_dem · 02 Sep 2019
> Recuperem la iniciativa!
> Amb la noviolència i la desobediència civil com a eines, avancem-nos a la sentència. Canviem l'estat de les coses:...
> Show this thread

02 de setiembre de 2019

**Josep Lluís Alay**
@josepalay

Que el Tsunami Democràtic s'endugui la injustícia i la repressió de casa nostra!

> **Tsunami Democràtic** @tsunami_dem · 02 Sep 2019
> Recuperem la iniciativa!
> Amb la noviolència i la desobediència civil com a eines, avancem-nos a la sentència. Canviem l'estat de les coses:...
> Show this thread

02 de setiembre de 2019

**Alfred Bosch**
@AlfredBosch

Contra els huracans de repressió, tsunamis democràtics. Benvinguts @tsunami_dem per respondre democràticament i pacíficament a una injustícia històrica.

> **Tsunami Democràtic** @tsunami_dem · 02 Sep 2019
> Recuperem la iniciativa!
> Amb la noviolència i la desobediència civil com a eines, avancem-nos a la sentència. Canviem l'estat de les coses:...
> Show this thread

02 de setiembre de 2019

**Roger Torrent i Ramió**
@Rogertorrent

Davant la involució democràtica de l'Estat, conjurem-nos per defensar els drets i llibertats des de la no violència. Votar mai pot ser un delicte!

**#TsunamiDemocràtic**

> **Tsunami Democràtic** @tsunami_dem · 02 Sep 2019
> Recuperem la iniciativa!
> Amb la noviolència i la desobediència civil com a eines, avancem-nos a la sentència. Canviem l'estat de les coses:...
> Show this thread

02 de setiembre de 2019

**krls.eth / Carles Puigdemont**
@KRLS

Cal recuperar la iniciativa, i en tots els àmbits. Aquesta és una bona manera, intel·ligent. El compromís amb la no violència ens fa més forts, que ningú en tingui cap dubte. I sí, ara comença el temps de la represa.

> **Tsunami Democràtic** @tsunami_dem · 02 Sep 2019
> Recuperem la iniciativa!
> Amb la noviolència i la desobediència civil com a eines, avancem-nos a la sentència. Canviem l'estat de les coses:...
> Show this thread

02 de setiembre de 2019

**Oriol Junqueras**
@junqueras

Junqueras: Votar no és delicte! La democràcia prevaldrà per sobre de tot i ens conjurem per defensar-la! Sempre!
**#tsunamidemocratic**

> **Tsunami Democràtic** @tsunami_dem · 02 Sep 2019
> Recuperem la iniciativa!
> Amb la noviolència i la desobediència civil com a eines, avancem-nos a la sentència. Canviem l'estat de les coses:...
> Show this thread

02 de setiembre de 2019

**Pere Aragonès i Garcia**
@perearagones

Votar, fer un referèndum no és cap delicte. Tampoc ho és la independència. Sortirem sempre i arreu a defensar-ho! La democràcia i la llibertat sempre, conjurem-nos!
**#TsunamiDemocràtic**

> **Tsunami Democràtic** @tsunami_dem · 02 Sep 2019
> Recuperem la iniciativa!
> Amb la noviolència i la desobediència civil com a eines, avancem-nos a la sentència. Canviem l'estat de les coses:...
> Show this thread

02 de setiembre de 2019

**Josep Costa**
@josepcosta

Ja m'hi he sumat. I vosaltres?

> **Tsunami Democràtic** @tsunami_dem · 02 Sep 2019
> Recuperem la iniciativa!
> Amb la noviolència i la desobediència civil com a eines, avancem-nos a la sentència. Canviem l'estat de les coses:...
> Show this thread

02 de setiembre de 2019

Por lo tanto, la presunta participación en actividades ilegales de tantos participantes voluntarios en el estudio CatalanGate personas a las que cualquier gobierno democrático tendría no solo el derecho, sino también la obligación de investigar- era pública y estaba bien documentada. Resulta extremadamente sorprendente que Citizen Lab no considerara como una posibilidad que estos participantes no fueran «víctimas», sino, por el contrario, miembros de una red que utilizaba medios ilegales en un proyecto secesionista e intentaba aprovechar la reputación del instituto de investigación canadiense para ayudar a disipar las acusaciones y las pruebas que se estaban recabando, en varias investigaciones judiciales y policiales en contra de ellos.

También es importante que algunas de las presuntas víctimas hicieran declaraciones públicas muy controvertidas durante el período en el que se llevó a cabo la investigación. Por ejemplo, la Sra. Paluzie, antigua dirigente de la organización secesionista ANC de 80.000 miembros, pidió abiertamente que se infringiera la ley y se implementara una declaración unilateral de independencia.[402] Del mismo modo, algunos de los líderes nacionalistas, considerados víctimas en el informe, afirmaron que «volverán a hacerlo» «ho tornarem a fer», refiriéndose al intento de intentar alcanzar unilateralmente la independencia de Cataluña.[403]

*402/* *Europa Press. PALUZIE (ANC) insta a preparar una DUI efectiva y ve «poco realista» pactar la autodeterminación, 5 de septiembre de 2021, https://www.europapress.es/catalunya/noticia-paluzie-anc-insta-preparar-dui-efectiva-ve-poco-realista-pactar-autodeterminacion-20210905110043.html*

*403/* *Cuixart, J. (2019). HO tornarem a fer. Quan la injustícia és la Llei, la desobediència civil és un DRET. Barcelona: ARA Llibres. Junqueras, O. Rovira, M. (2020), Tornarem a vencer (i com ho farem). Barcelona: ARA Llibres. La República. [Vídeo] Cuixart: «HO tornarem a fer i no en tinc cap dubte, perquto l'única lluita que es perd és la que s' abandona», 11 de julio de 2020, https://www.larepublica.cat/noticies/video-cuixart-ho-tornarem-a-fer-i-no-en-tinc-cap-dubte-perque-lunica-lluita-que-es-perd-es-la-que-sabandona/*

*Los Yellows Catalunya. Los Yellows 21 — Ho ternarem a fer. YouTube. 17 de junio de 2019, https://youtu.be/yqjIyscbi7o*

La mayoría de las presuntas víctimas del espionaje ilegal se encontraban investigados, haciendo frente o en espera de juicio o ya habían condenados por diversos delitos, en su mayor parte relacionados con el intento de conseguir la independencia de Cataluña por medios ilegales. Muchos de ellos tenían fuertes vínculos directos con otros participantes que formaban una red de activistas políticos antes y durante el período de investigación de CatalanGate. Esta red estaba intentando provocar una secesión unilateral de Cataluña apoyándose en medios que los tribunales españoles habían declarado ilegales en repetidas ocasiones, y a veces no constitucionales, y presumiblemente con apoyo de los servicios secretos rusos. Los protocolos éticos de investigación comúnmente aceptados sugieren el planteamiento de varias preguntas para evaluar si se trata de un caso de mala conducta en la investigación, con posibles efectos indirectos jurídicos en España:

A → *¿Se informó a la Universidad de Toronto de que muchos de los participantes estaban siendo juzgados o tenían órdenes de detención ante la justicia española antes de que se pusieran en contacto por primera vez con ellos?*

B → *¿Autorizó la Universidad de Toronto a Citizen Lab a advertir a los líderes secesionistas de la supuesta vigilancia por parte de los servicios de seguridad españoles?*

C → *¿Pidió Citizen Lab a los participantes en la investigación que mantuvieran la confidencialidad principal y solo advirtió a las personas seleccionadas por el equipo para evitar injerencias en el curso de la justicia en España?*

D → *¿Ha manifestado algún miembro de Citizen Lab su preocupación por el hecho de que su participación en la citada red de líderes secesionistas pudiese tener un impacto negativo en la estabilidad de España?*

E → *¿Existe algún protocolo ético o de seguridad específico en la Universidad de Toronto relativo a la participación en la investigación de sujetos sospechosos o investigados formalmente por cometer actividades delictivas?*

F → *¿Se comunicaron los cargos penales conocidos de los participantes al Consejo de Ética de la investigación?*

La Universidad de Toronto aún no ha dado respuesta a estas preguntas y las elusivas respuestas a estas cuestiones tan graves parecen indicar que no se aplicaron medidas cautelares provisionales durante el trabajo de campo en Cataluña.

## TABLA 5



## "VÍCTIMAS" CATALANGATE

| Lista de presuntas víctimas de Citizen Lab | | Web Catalangate.cat | Fugitivos de la justicia con órdenes internacionales | Vigilancia con autorización judicial[1] | Condenado a prisión | Implicado en investigaciones policiales o juicios | Relación personal con activistas y políticos investigados |
|---|---|---|---|---|---|---|---|
| Jordi Cuixart | Activista político y antiguo líder de la organización secesionista Òmnium | Jordi Cuixart | | | Jordi Cuixart condenado a 9 años por sedición[2] | | Pareja de Meritxell Bonet. Amigo de Junqueras, Puigdemont y Jordi Sànchez, entre otros |
| Carles Puigdemont | Expresidente de la Generalitat (Junts per Catalunya) | Carles Puigdemont | Carles Puigdemont | Carles Puigdemont | | Investigado por rebelión y apropiación indebida de fondos públicos, así como por la organización de Tsunami Democràtic[3] | Miembro del Gobierno catalán que declaró la independencia unilateral |
| Oriol Junqueras | Expresidente de la Generalitat (ERC) | Oriol Junqueras | | Oriol Junqueras | Oriol Junqueras condenado a 13 años por sedición y malversación.[4] | | Miembro del Gobierno catalán que declaró la independencia unilateral |
| Alba Bosch | Activista política | Alba Bosch | | | | | |
| Albano Dante Fachin | Político (antiguo Podem y Front Republica), activista y periodista | Albano Dante Fachin | | | | | Amigo de Puidgemont, Jon Inarritu, Toni Comin, etc.[5] |
| Albert Batet | Político (Junts per Catalunya) | Albert Batet | | Albert Batet | | | Amigo personal de Carles Puigdemont |
| Albert Botran | Político (CUP)/ Diputado del Congreso Español y miembro de la comisión de Secretos Oficiales. | Albert Botran | | | | Albert Botran (investigado en 2017 por participar en un homenaje al grupo terrorista Terra Lliure)[6] | Fernández, Riera y Botran presentaron una denuncia conjunta en relación con Pegasus. Fernández y Botran han colaborado en varias ocasiones |
| Andreu Van den Eynde | Abogado de Oriol Junqueras y Raül Romeva y activista político | Andreu Van den Eynde | | | | | Amigo de David Fernández. Amigo y abogado de Roger Torrent[7] |
| | | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Anna Gabriel | Política (CUP)/ primera política no miembro del Gobierno catalán que firma la Declaración Uniforme de Independencia | Anna Gabriel | Anna Gabriel | | | Anna Gabriel investigada por el Tribunal Supremo por cargos de rebelión y por la Audiencia Nacional por su relación con los CDRs[8] | Estrecha colaboradora de Riera |
| Antoni Comín | Político (ERC) | Antoni Comín | Antoni Comín | | | Antoni Comin investigado por el Tribunal Supremo por acusaciones de rebelión y por su rol en el asunto «Voloh»[9] | Amigo y colaborador estrecho de Puigdemont |
| Arià Bayé | Activista político, miembro de la organización secesionista ANC | Arià Bayé | | | | Arià Bayé fue arrestado por su participación en disturbios violentos, fue absuelto en 2021[10] | Paluzie, Domingo, Urpi y Sànchez presentaron una denuncia formal conjunta contra NSO |
| Arnaldo Otegi | Líder de EH Bildu/ antiguo miembro del grupo terrorista ETA | | | | Arnaldo Otegui fue condenado a 10 años por ser miembro de ETA, liberado en 2016[11] | | |
| Artur Mas | Político (CDC y PDeCAT) ex Presidente de Cataluña | Artur Mas | | | | Artur Mas fue condenado por desobediencia y considerado corresponsable de devolver 5 millones de euros gastados en el referéndum ilegal de 9N en 2014[12] | Artur Mas eligió a Puigdemont como su sucesor |
| Carles Riera | Político (CUP) | Carles Riera | | Carles Riera | | Se investigó a Carles Riera en relación con las protestas violentas de Tsunami Democràtic[13] | Colaborador estrecha de Gabriel |
| David Bonvehi | Político (PDeCAT) | | | David Bonvehi | | | Hasta 2020 colaboraba estrechamente con Puigdemont |
| David Fernández | Político (CUP). Acuñó el término « Tsunami Democràtic» en 2014 en relación con el referéndum ilegal de independencia de 9N. | David Fernández | | | | Se investigó a David Fernandez en relación con las protestas violentas del Tsunami Democratic[14] | Amigo personal de Cuixart. Fernández, Riera y Botran presentaron una denuncia conjunta en relación con Pegasus. Fernández y Botran han colaborado en numerosas ocasiones. |

## TABLA 5



## "VÍCTIMAS" CATALANGATE

| Lista de presuntas víctimas de Citizen Lab | | Web Catalangate.cat | Fugitivos de la justicia con órdenes internacionales | Vigilancia con autorización judicial[1] | Condenado a prisión | Implicado en investigaciones policiales o juicios | Relación personal con activistas y políticos investigados |
|---|---|---|---|---|---|---|---|
| David Madi | Político (Junts per Catalunya) y empresario | David Madi | | | David Madi condenado a 14 meses por cargos de fraude[15] | David Madi fue detenido e investigado en el "caso Voloh"[16] | Amigo personal de Puigdemont |
| Diana Riba | Política (ERC). Vicepresidenta de la Comisión de Pegasus en el Parlamento Europeo | Diana Riba | | | | | Esposa del líder secesionista encarcelado y después indultado, Raül Romeva. Jordi Sole, Josep Maria Jove y Diana Riba presentaron una queja formal contra el NSO. |
| Dolors Mas | Empresaria | Dolors Mas | | | | | Amiga de Puigdemont |
| Dr. Elias Campo | Padre de Elias Campo y médico | Dr. Elias Campo | | | | | Padre de Elies Campo y marido de Maria Cid |
| Elias Campo | Empresario y activista, autor del informe CatalanGate y *fellow* de Citizen Lab | Elias Campo | | | | Se investigó a Elies Campo por participar en la creación de la aplicación Tsunami Democràtic[17] | Autor del informe, colaboró con Xavier Vives, Jordi Baylina, Pau Escrich, Puigdemont |
| Elisenda Paluzie | Activista política, expresidenta de la ANC | Elisenda Paluzie | | Elisenda Paluzie | | Elisenda Paluzie fue investigada por justificar en televisión el uso de vilolencia por la causa pro-independencia[18] | Paluzie, Domingo, Urpi y Sànchez presentaron una denuncia formal conjunta contra NSO. |
| Elsa Artadi | Política (Junts per Catalunya) | Elsa Artadi | | Elsa Artadi | | Elsa Artadi fue investigada por sus reuniones secretas con los emisarios del Kremlin antes de la declaración de independencia y el "CNI catalán"[19] | Colaboradora estrecha de Puigdemont[20] |
| | | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Ernest Maragall | Político (ERC) | Ernest Maragall | | | | | Acuñó el término CatalanGate. Ernest Maragall y Roger Torrent presentaron una denuncia formal conjunta sobre el presunto espionaje con Pegasus. |
| Ferran Bel | Político (PDeCAT) | Ferran Bel | | | | Ferran Bel fue investigado por participar en la organización del referéndum ilegal de 2017[21] | Colaborador de Puigdemont[22] |
| Gonzalo Boye | Abogado de Carles Puigdemont y muchos otros líderes secesionistas/antiguo condenado por colaboración con el grupo terrorista ETA | Gonzalo Boye | | Gonzalo Boye | Encarcelado por cargos terroristas pero liberado en 2002 | Gonzalo Boye fue investigado por blanqueo de dinero para una organización de tráfico de drogas[23] | Colaborador estrecho y amigo personal de Puigdemont. Coordinador del proceso de identificación de presuntas víctimas en Junts por Catalunya |
| Jaume Alonso Cuevillas | Político (Junts per Catalunya) y abogado de Carles Puigdemont y otros líderes secesionistas | Jaume Alonso Cuevillas | | | | | Colaborador estrecho de Puigdemont[24] |
| Joan Matamala | Empresario y activista | Joan Matamala | | Joan Matamala | | Se investigó a Joan Matamala por participar en la creación de la aplicación Tsunami democràtic[25] | Personal friend of Carles Puigdemont. Collaborator of Jordi Baylina |
| Joan Ramon Casals | Político (Junts per Catalunya) | Joan Ramon Casals | | | | Joan Ramon Casals was investigated for participating in the organisation of the illegal referendum in 2017[26] | Colaborador de Joaquim Torra |
| Joaquim Jubert | Político (Junts per Catalunya) | Joaquim Jubert | | | | | Collaborator of Jordi Sànchez |
| Joaquim Torra | Político (Junts per Catalunya), expresidente de | Joaquim Torra | | | | Joaquim Torra fue investigado y condenado por desobediencia[27] | Colaborador de Puigdemont quien le nombró sucesor[28] |
| Jon Iñarritu | Político (EH Bildu) | Jon Iñarritu | | | | | Amigo de Puigdemont, Comin, Dante Fachin, etc.[29] |

## TABLA 5



## "VÍCTIMAS" CATALANGATE

| Lista de presuntas víctimas de Citizen Lab | | Web Catalangate.cat | Fugitivos de la justicia con órdenes internacionales | Vigilancia con autorización judicial[1] | Condenado a prisión | Implicado en investigaciones policiales o juicios | Relación personal con activistas y políticos investigados |
|---|---|---|---|---|---|---|---|
| Jordi Baylina | Emprendedor y activista político de TI | Jordi Baylina | | Jordi Baylina | | Jordi Baylina fue investigado por participar en la creación de la aplicación de Tsunami democràtic[30] | Socio de Sonia Urpí. Colaboró con Xavi Vives, Pau Escrich y Elies Campo. Colaboró con Puigdemont y Joan Matamala. |
| Jordi Bosch | Activista político miembro del secesionista Òmnium | | | Jordi Bosch | | | Amigo personal y colaborador de Jordi Cuixart |
| Jordi Domingo | Activista político miembro de la ANC secesionista | Jordi Domingo | | | | Jordi Domingo fue investigado por su participación en la creación del "CNI Catalán"[31] | Paluzie, Domingo, Urpi y Sànchez presentaron una denuncia formal conjunta contra NSO. |
| Jordi Sànchez | Político (Junts per Catalunya) y antiguo líder de la organización secesionista ANC | Jordi Sànchez | | Jordi Sànchez | Sentencia Jordi Sànchez a 9 años para la sediciónn[32] | | Paluzie, Domingo, Urpi y Sànchez presentaron una denuncia formal conjunta contra NSO. |
| Jordi Solé | Político (CEI) | Jordi Solé | | | | | Jordi Solè, Josep Mª Jove y Diana Riba presentaron una denuncia formal conjunta contra NSO. |
| Josep Costa | Político (Junts per Catalunya) | Josep Costa | | | | Josep Costa fue investigado y detenido por desobediencia[33] | Colaborador estrecho de Puigdemont |
| Josep Lluis Alay | Político (Junts per Catalunya) | Josep Lluis Alay | | Josep Lluis Alay | | Josep Lluis Alay fue investigado en el caso Voloh por cargos de corrupción[34] | Colaborador estrecho de Puigdemont |
| | | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Josep Maria Ganyet | Emprendedor y activista político de TI | Josep Maria Ganyet | | | | Josep Maria Ganyet fue investigado por su participación en la creación del «CNI catalán» y la aplicación Tsunami Democratic.[35] | Colaboró con Torra |
| Josep Maria Jové | Político (ERC) | Josep Maria Jové | | | | Josep Maria Jove fue detenido e investigado por coordinar la logística del referéndum ilegal de 2017[36] | Estrecho colaborador de Oriol Junqueras. Jordi Solè, Josep Mª Jove y Diana Riba presentaron una denuncio formal conjunta contra el NSC |
| Josep Rius | Político (Junts per Catalunya) | Josep Rius | | | | | Colaborador estrecho de Puigdemont[37] |
| Laura Borràs | Política (Junts per Catalunya) | Laura Borràs | | | | Investigada por acusaciones de corrupción[38] | Colaboradora estrecha de Torra[39] |
| Marc Solsona | Político (PDeCAT) | Marc Solsona | | | | Marc Solsona fue investigado por participar en la organización del referéndum ilegal de 2017[40] | |
| Marcel Mauri | Activista político, vicepresidente de Òmnium | Marcel Mauri | | Marcel Mauri | | Marcel Mauri fue investigado en relación con las protestas violentas del Tsunami. | |
| Marcela Topor | Periodista | Marcela Topor | | | | | Esposa de Carles Puigdemont |
| Maria Cinta Cid | Consultora sanitaria | Maria Cinta Cid | | | | | Madre de Elies Campo y esposa del Dr. Elias Campo |
| Marta Pascal | Política (PNC former PDeCat) | Marta Pascal | | | | Marta Pascal fue investigada por el Tribunal Supermo por rebelión y desobediencia, pero no fue procesada.[41] | Marta Pascal colaboró estrechamente con Mas, pero a menudo se opuso a Puigdemont |

## TABLA 5



## "VÍCTIMAS" CATALANGATE

| Lista de presuntas víctimas de Citizen Lab | | Web Catalangate.cat | Fugitivos de la justicia con órdenes internacionales | Vigilancia con autorización judicial[1] | Condenado a prisión | Implicado en investigaciones policiales o juicios | Relación personal con activistas y políticos investigados |
|---|---|---|---|---|---|---|---|
| Marta Rovira | Política (ERC) | Marta Rovira | Marta Rovira | | | Marta Rovira fue investigada por el Tribunal Supremo por rebellón y desobediencia[42] | Miembro del Gobierno catalán que declaró la independencia unilateral |
| Meritxell Bonet | Periodista y activista política de Òmnium/ socia de Jordi Cuixart | Meritxell Bonet | | | | | Socia de Jordi Cuixart, líder secesionista encarcelado y posteriormente perdonado |
| Meritxell Budó | Política (Junts per Catalunya) | Meritxell Budó | | | | Meritxell Budó fue investigada en un caso de corrupción[43] | Estrecha colaboradora de Torra |
| Meritxell Serret | Política (ERC) | Meritxell Serret | Meritxell Serret | | | Meritxell Serret fue investigada por desobediencia[44] | Miembro del Gobierno catalán que declaró la independencia unilateral |
| Miriam Nogueras | Política (Junts per Catalunya) /Diputada del Congreso, miembro de la comisión de Secretos Oficiales. | Miriam Nogueras | | | | | |
| Oriol Sagrera | Político (ERC) | Oriol Sagrera | | | | | Colaboradora cercana de Roger Torrent. Colaboradora de Van den Eynde |
| Pau Escrich | Empresario y activista político de tecnologías de la información | Pau Escrich | | Pau Escrich | | Se investigó a Pau Escrich por su participación en la creación de la aplicación Tsunami Democràtic.[45] | Colaboró con Xavi Vives, Jordi Baylina y Elies Campo |
| | | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Pere Aragonès | Político (ERC), Presidente de Cataluña | Pere Aragonès | | Pere Aragonès | | Se investigó a Pere Aragonès por la organización del referéndum ilegal de 2017[46] | Colaborador de Oriol Junqueras, quién le nombró sucesor |
| Pol Cruz | Activista político de Òmnium | Pol Cruz | | | | | Colaborador de Puigdemont |
| Roger Torrent | Político (ERC) | Roger Torrent | | | | Roger Torrent fue investigado por desobediencia. También fue acusado por el Tribunal Constitucional de infringir los derechos de los diputados catalanes de la oposición[47] | Ernest Maragall y Roger Torrent presentaron una denuncia formal conjunta sobre el presunto espionaje con Pegasus |
| Sergi Miquel | Político (PDeCAT) | Sergi Miquel | | Sergi Miquel | | Sergi Miquel fue investigado por su participación en la creación de la aplicación Tsunami Democràtic[48] | Colaborador de Puigdemont |
| Sergi Sabrià | Político (ERC) | Sergi Sabrià | | | | | Colaborador de Pere Aragonès |
| Sònia Urpí | Activista político miembro de la ANC secesionista | Sònia Urpí | | | | | Urpi es el socio de Baylina. Plauzie, Domingo, Urpi y Sànchez presentaron una denuncia formal conjunta contra NSC |
| Xavier Vendrell | Político (ERC) y emprendedor. Presunto líder de Tsunami Democràtic. Antiguo miembro del grupo terrorista Terra Lliure | Xavier Vendrell | | Xavier Vendrell | | Xavier Vendrell fue investigado en “Voloh”, por su implicación en el Tsunami y presuntas acusaciones de corrupción[49] | Oriol Junqueras seleccionó a Vendrell para coordinar la estrategia para organizar el referéndum[50] |
| Xavier Vives | Emprendedor y activista político de TI | Xavier Vives | | Xavier Vives | | Xavier Vives fue investigado por su participación en la creación de la aplicación Tsunami Democràtic[48] | Colaboró con Jordi Baylina, Pau Escrich y Elies Campo |
| Clara Ponsatí | Política (Junts per Catalunya) | | Clara Ponsatí | | | Clara Ponsatí fue investigada por rebelión y malversación de fondos públicos[52] | Colaboró con Jordi Baylina, Pau Escrich y Elies Campo |

1/ https://www.lavanguardia.com/politica/20220505/8243657/caso-pegasus-espionaje-cni-paz-esteban-congreso-comision-ultimas-noticias-hoy-en-directo.html

2/ https://www.ccma.cat/324/jordi-cuixart-y-jordi-sanchez-condenados-a-9-anos-de-carcel-por-sedicion/noticia-es/2955685/

3/ https://www.eldiario.es/catalunya/puigdemont-principal-carpeta-proces-tribunales-espera-desjudicializacion_1_9581694.html

4/ https://www.lavanguardia.com/politica/20191014/47901758567/oriol-junqueras-sentencia-1o-caso-proces-condena.html

5/ https://www.lavozdeasturias.es/noticia/actualidad/2021/07/28/rahola-reune-puigdemont-circulo-amigos-paella-verano-celebro-2016/00031627468522266533659.htm

6/ https://www.elespanol.com/espana/20220428/botran-investigado-enaltecer-terrorismo-defensor-putin-cni/668433543_0.html

7/ https://www.ccma.cat/tv3/alacarta/preguntes-frequents/99-la-nova-banda-de-rock-dandreu-van-den-eynde/video/6122106/

8/ https://magnet.xataka.com/en-diez-minutos/anna-gabriel-y-su-huida-a-ginebra-de-que-le-acusa-el-supremo-y-que-dicen-las-leyes-suizas

9/ https://www.larazon.es/espana/20210615/tblls6o2mvfwphefqz233vwgsq.html

10/ https://unilateral.cat/2017/05/08/detinguts-4-membres-del-sindicat-destudiants-sepc/

11/ https://kangaroo.vocento.com/tr-pixel.gif?continue=https://www.abc.es/espana/abci-cuales-delitos-otegui-sido-condenado-201906271122_noticia.html&ref=

12/ https://www.elmundo.es/espana/2021/10/06/615da5de21efa0ff2b8b461b.html

13/ https://www.antena3.com/noticias/espana/salen-luz-nuevos-nombres-politicos-independentistas-espiados-autorizacion-cni_20220506627570 09eb0a930001cccc8d.html

14/ https://www.elconfidencial.com/espana/2019-10-18/puigdemont-cup-informaticos-1o-mueven-hilos-tsunami-democratic-852_2288811/

15/ https://www.elmundo.es/cataluna/2022/10/25/63581f1121efa0361d8b4593.html

16/ https://www.elperiodico.com/es/politica/20210520/jueza-david-madi-caso-3-facturas-falsas-11746090

17/ https://www.elperiodico.com/es/politica/20210621/guardia-civil-vendrell-madi-tsunami-11844090

18/ https://www.lavanguardia.com/politica/20191106/471426260395/fiscalia-investiga-elisenda-paluzie-anc-violencia-declaraciones.html

19/ https://www.vozpopuli.com/espana/guardia-civil-reuniones-cni-catalan-elsa-artadi.html

20/ https://www.elconfidencial.com/espana/cataluna/2021-07-03/manda-junts-jordi-sanchez-maniobra-partido_3164939/

21/ https://elpais.com/politica/2017/09/19/actualidad/1505825351_174090.html

22/ https://ebredigital.cat/2017/11/14/ferran-bel-va-assessorar-a-puigdemont-per-presentar-se-amb-junts-per-catalunya/

23/ https://www.eldiario.es/politica/audiencia-nacional-confirma-procesamiento-blanqueo-gonzalo-boye-abogado-puigdemont_1_8081620.html

24/ https://www.elconfidencial.com/espana/cataluna/2021-07-03/manda-junts-jordi-sanchez-maniobra-partido_3164939/

25/ https://www.elperiodico.com/es/politica/20210621/guardia-civil-vendrell-madi-tsunami-11844090

26/ https://www.vilapress.cat/texto-diario/mostrar/1436394/ex-alcalde-molins-joan-ramon-casals-exalcalde-molins-investigado-desobediencia-1

27/ https://www.elperiodico.com/es/politica/20220511/torra-condenado-pancarta-generalitat-13640287

28/ https://elpais.com/ccaa/2018/05/10/catalunya/1525973613_424317.html

29/ https://www.lavozdeasturias.es/noticia/actualidad/2021/07/28/rahola-reune-puigdemont-circulo-amigos-paella-verano-celebro-2016/00031627468522266533659.htm

30/ https://www.elperiodico.com/es/politica/20210621/guardia-civil-vendrell-madi-tsunami-11844090

31/ https://www.20minutos.es/noticia/5070783/0/la-guardia-civil-situa-a-empresarios-e-informaticos-en-el-cni-catalan-que-se-reunio-con-cdr-para-aupar-la-republica/

32/ https://www.ccma.cat/324/jordi-cuixart-y-jordi-sanchez-condenados-a-9-anos-de-carcel-por-sedicion/noticia-es/2955685/

33/ https://www.lavanguardia.com/politica/20211027/7819603/detenido-josep-costa-comparecer-tsjc.html

34/ https://www.elconfidencial.com/espana/cataluna/2022-04-20/juez-investiga-patrimonio-alay_3411694/

35/ https://www.elperiodico.com/es/politica/20210621/guardia-civil-vendrell-madi-tsunami-11844090

36/ https://www.lavanguardia.com/politica/20180214/44785003439/guardia-civil-jove-cerebro-ejecutor-1o-ordenes-junqueras-marta-rovira.html

37/ https://www.elconfidencial.com/espana/cataluna/2021-07-03/manda-junts-jordi-sanchez-maniobra-partido_3164939/

38/ https://www.eldiario.es/catalunya/juez-procesa-laura-borras-corrupcion-acelera-salida-parlament_1_9128940.html

39/ https://www.elconfidencial.com/espana/cataluna/2021-07-03/manda-junts-jordi-sanchez-maniobra-partido_3164939/

40/ https://elpais.com/ccaa/2017/09/19/catalunya/1505805699_062547.html

41/ https://www.eldiario.es/politica/artur-marta-pascal-neus-lloveras_1_2774360.html

42/ https://www.elindependiente.com/politica/2018/02/19/marta-rovira-libertad-fianza-declarar-supremo/

43/ https://cadenaser.com/ser/2019/11/17/tribunales/1573979444_137427.html

44/ https://www.niusdiario.es/espana/catalunya/20220919/fiscalia-pide-diputada-erc-meritxell-serret-inhabilitada-un-ano-desobediencia-referendum_18_07487545.html

45/ https://www.elperiodico.com/es/politica/20210621/guardia-civil-vendrell-madi-tsunami-11844090

46/ https://www.lavanguardia.com/politica/20180808/451251546147/juez-1o-barcelona-tsjc-investigue-pere-aragones.html

47/ https://www.eldiario.es/catalunya/puigdemont-principal-carpeta-proces-tribunales-espera-desjudicializacion_1_9581694.html

48/ https://es.ara.cat/politica/gobierno-sanchez-autorizo-espionaje-18-dirigentes-tsunami-democratic-confidencial_1_4353964.html

49/ https://www.elperiodico.com/es/politica/20210621/guardia-civil-vendrell-madi-tsunami-11844090

50/ https://www.catalunyapress.es/texto-diario/mostrar/732534/junqueras-repesca-puigcercos-vendrell

51/ https://www.elperiodico.com/es/politica/20210621/guardia-civil-vendrell-madi-tsunami-11844090

52/ https://www.eleconomista.es/politica/noticias/9034710/03/18/15/Ponsati-se-entregara-el-miercoles-en-una-comisaria-de-Edimburgo.html

# 15

# Los colaboradores de Citizen Lab intentan silenciar al autor de este informe

El autor de este informe ha hecho frente a una campaña que intentó deslegitimarlo públicamente desde que empezó a descubrir las deficiencias de la investigación catalana que se han mostrado anteriormente (cuadro). La prensa española tomó nota de esta campaña de difamación en julio de 2022[404]. Hay muchas evidencias de estos intentos de desacreditar su trabajo en redes sociales:

*404/* *El Triangle. El entorno de Citizen Lab lanza una campaña de insultos en Twitter contra quienes cuestionan su «CatalanGate» 25 de julio de 2022, https://www.eltriangle.eu/es/2022/07/25/el-entorno-de-citizen-lab-lanza-una-campana-de-insultos-en-twitter-contra-quienes-cuestionan-su-catalangate/*

**Jens Wiechers**
@jwiechers

Replying to **@MalwareTechBlog**

I think the Spaniard is just an ultranationalist, which even people with PhDs can be, sadly. That should motivate his reasoning. The journalist I get more of a paid comms interference vibe from, from looking through her past stuff, too.

**Feed me scanlines** @devnetse...

Replying to **@MalwareTechBlog**

Juan José is an ultranationalist that would go to great lengths to fuck with Catalans. He's just riding this wave and paid by other people.

**Feed me scanlines** @devnetse...

Sorry, Jose Javier. I need some help :)

**Lukasz** @maldr0id

Replying to **@MalwareTechBlog @joseolivas and 2 others**

Thats what I don't get either. They aren't very good at their job and I assume that whoever pays them probably has enough money to pay someone better.

That being said **@elconfidencial** has published an article yesterday citing Jose and Jonathan.

**Mark Owen Jones** @marcowenjones

hmm interesting, of course this is what they want. Do you have a link to the article?

**Lukasz** @maldr0id

Replying to **@marcowenjones @joseolivas and 3 others**

Here you go:

**RAGEPATH** @ragepath

Replying to **@ragepath @joseolivas and 4 others**

Not saying that's what going on here. But like, captive academics of the fossil fuel industry and tobacco industry convince¡ced a lot of people there is a good value proposition to investing in fraudulent academic credentialism as a long con.

**Marcus Hutchins**
@MalwareTechBlog

Replying to **@ragepath @joseolivas and 3 others**

I'd bet $100 someone is paying Jose off. His initial thread and the later attempt to dismiss all criticism with "they're  all just friends of citizenlab" is giving me big paid stooge energy.

9:04 · 17 de julio de 2022

**profdeibert**
@RonDeibert

Replying to **@joseolivas**

The main (and thoroughly debunked) "evidentiary" source for the far-right, pro-spain disinformation campaign making false & defamatory charges against @citizenlab and me is now comparing our methods to Nazis and asserting crop circles are due to secret US military experiments...1/

17:03 · 14 de julio de 2022

**Marcus Hutchins**
@MalwareTechBlog

Replying to **@joseolivas**

Imagine having so little credibility that your argument is literally "the only guy making this claim must be correct and everyone opposing it is just friends of the person the claim is against". I want to tell myself you're just a moron, but I'm pretty sure you're NSO payroll

18:20 · 16 de julio de 2022

**Marc Owen Jones** @marcowenjones

It's a very key point. One has to wonder why @irinatsukerman_ and @joseolivas are really doubling down the work of a discredited and unethical hacker doing apologetics for NSO Group. Literally selecting the bad source among the good ones is unacademic

> **Marcus Hutchins** @MalwareTechBlog
> Replying to **@joseolivas**
> Ok, let's talk about pre existing bias. You took the only, and I mean only, researcher holding such hostile views towards those entities and ignored his complete lack of credibility and skill because it reinforced your point. You are a stooge.

19:16 · 05 de mayo de 2022

**Marcus Hutchins** @MalwareTechBlog
Replying to **@jonathandata0**
[Jose Javier Olivas is typing]

**The Old Guard** @jonathandata0
Another example of not ad hominem: Jose you're a tool. Eat my ass.

**Infosec Nietzsche** @nihlsec

Replying to **@joseolivas @jonathandata1 and 4 others**

Well José maybe you're the useful idiot in this case, as Jonathan appears to be using your credentials and sharing of his work as validation for it's accuracy whereas you were only sharing it out of interest as it aligns with your conclusions regarding Citizen Labs work.

**Marc Owen Jones** @marcowenjones

Replying to **@joseolivas @jonathandata1 and 2 others**

No shit. And from the person with a very ostentatious LSE logo in the background of a profile pic. Methinks thou doth protest too much

16:49 · 15 de julio de 2022

Del mismo modo, un influyente experto en seguridad digital, Nadim Kobeissi, también denunció esta campaña.[405]

**Nadim Kobeissi (@nadim@symbolic.so...**
@kaepora

A number of researchers (**@joseolivas**), **@irinatsukerman_** etc) have been pointing out the bankrupt scientific methodology that Citizen Lab have been applying to their forensic reports, only to be met with predictable Twitter ad-hominem etc. As a reminder, my thread fro last year:

> **Nadim Kobeissi (@nadim@symbolic...** @MalwareTec...
> I decided to give the recent Pegasus coverage the benefit of the doubt and spent my lunch break looking up other reports by the same folks.
>
> In a report published last week, their "only" evidence for attribution is a "self-signed" TLS certificate. That's not evidence.

20 de julio de 2021

El lunes 21 de noviembre de 2022 se envió una carta difamatoria a los miembros de la Comisión de Investigación PEGA del Parlamento Europeo para intentar vetar el testimonio del autor de este informe en una audiencia prevista para el 28 de noviembre de 2022, a la que ya había sido invitado y confirmado como participante el viernes 18 de noviembre de 2022. La carta se redactó rápidamente después de que un miembro de la Comisión PEGA filtrara a CitizenLab la información que recogía la participación del autor de esta revisión crítica. Esta carta difamatoria incluye una serie de acusaciones graves e infundadas que, al parecer, estaban destinadas a socavar su credibilidad profesional.

*405/* *Nadim Kobeissi, @kaepora, 18 de julio de 2022, https://twitter.com/kaepora/status/1549007373175586818?s=20&t=QqTUVTSiNKHW2s8Q-7vE9rw*

Por ejemplo, en esta carta se afirma que el autor de este informe:

«Participa en un patrón de acoso a investigadores y víctimas. Esto incluye la promoción de teorías conspiratorias y falsas denuncias sobre investigadores, víctimas de programas espía como Carine Kanimba e instituciones. Promueve sistemáticamente afirmaciones técnicas falsas, a pesar de haber sido informado por los expertos de su falsedad» y de que «forma parte de una campaña de desinformación más amplia para desacreditar el trabajo de organizaciones de confianza contra los programas espía y desviar a la comisión de su misión de investigación. Creemos que ofrecer a cualquiera de estas personas una plataforma en PEGA seguirá propagando campañas de desinformación organizadas y acoso a las víctimas de programas espía, y disuadirá a las víctimas de testificar en el futuro».

La carta difamatoria también se envió a grandes medios como The Guardian, Euractiv y Politico, presumiblemente para dar la mayor publicidad posible a las acusaciones y predisponer al público contra las pruebas que el autor de esta revisión crítica recabó durante meses de investigación independiente del caso CatalanGate.

The Guardian[406] invitó al autor de este informe a compartir su opinión sobre las acusaciones, y tanto Euractiv[407] como Politico[408] decidieron modificar los artículos que habían publicado inicialmente, una vez que el autor de esta revisión se puso en contacto con ellos. Todas las entidades y personas que supuestamente firmaron y enviaron la carta difamatoria contra el autor de este informe Access Now, Article 19, Digital Rights Foundation, Electronic Frontier Foundation, Human Rights Foundation, Red en Defensa de los Derechos Digitales (R3D), Red Line for Gulf (RL4G), tienen una estrecha relación de trabajo con Citizen Lab.[409] El autor y su abogado han solicitado a las instituciones firmantes la confirmación de la autoría de la carta difamatoria, pero ninguna de ellas ha respondido confirmando o rechazando su participación en la carta. Es muy poco probable que estas organizaciones tuvieran tiempo de llevar a cabo un debate interno mínimo y decidir apoyar una acción tan polémica durante un fin de semana. El autor de esta revisión no tiene conocimiento de ningún intento de confirmación de la autoría de la carta por parte de la Secretaría de la Comisión PEGA.

Cabe señalar que el 23 de noviembre de 2021 el Sr. John Scott-Railton celebró el anuncio formal de la denuncia judicial de Apple contra NSO con un hilo de Twitter en el que, entre otras cosas, felicitó a varias de las demás organizaciones que supuestamente firmaron la carta difamatoria por su contribución para recoger pruebas contra NSO.

*406/* *The Guardian. Pegasus spyware inquiry targeted by disinformation campaign, say experts. 28 de noviembre de 2022, https://www.theguardian.com/world/2022/nov/28/pegasus-eu-parliament-spyware-inquiry-targeted-disinformation-campaign. This article was signed by Ms Kirchgaessner and Mr Jones, who presumably received the defamatory letter from Citizen Lab.*

*407/* *Euractiv. EU Parliament's spyware investigation on Spain continues to spur controversy. 24 de noviembre de 2022 (actualizado el 28 de noviembre de 2022) https://www.euractiv.com/section/digital/news/eu-parliaments-spyware-investigation-on-spain-continues-to-spur-controversy/*

*408/* *Politico. EU spyware probe has a problem: Spain. Updated 28 de noviembre de 2022, https://www.politico.eu/article/eu-spyware-probe-problem-spain-pedro-sanchez-margaritas-robles/*

*409/* *Muchos de los firmantes también fueron invitados a comparecer en comisión, como el Sr. Ben Wagner, la Sra. Cindy Cohn, la Sra. Carine Kanimba y el Sr. David Kaye.*

«Considero que la demanda de @Apple se debe en parte a los resultados de los esfuerzos de tantos de nuestros compañeros de @citizenlab: Por ejemplo, @AmnestyTech @accessnow @RSF_inter @EFF @pressfreedom @R3Dmx @article19org y otros muchos».[410]

Como se ha explicado en una sección anterior, el Sr. Deibert es uno de los cinco miembros del comité de la Fundación Ford que decide la asignación de la recompensa de 10 millones de dólares que Apple ha destinado a las organizaciones que, como afirma el Sr. Scott-Railton, han colaborado en la recogida de pruebas incriminatorias contra NSO para el gigante Cupertino[411]. Estas organizaciones pueden haberse sentido obligadas a apoyar la carta de Citizen Lab y de vetar el testimonio del autor de este informe, o al menos no rechazar formalmente su participación en ella, dado que el Sr. Deibert es una figura clave en la asignación de la financiación de Apple. El hecho de que ninguna de las supuestas organizaciones firmantes haya confirmado o denegado su apoyo a la carta difamatoria sugiere la posibilidad de que no la respaldaran institucionalmente, pero podrían tener miedo de rechazar públicamente la autoría, ya que se vería perjudicada la reputación del Sr. Deibert.

*410/* *John Scott-Railton, @jsrailton, Twitter, 23 de noviembre de 2021; Tread stored in TreadReaderApp* *https://threadreaderapp.com/thread/1463206324704059401.html*

*411/* *Apple. Newsroom. Apple expands industry-leading commitment to protect users from highly targeted mercenary spyware. 6 de julio de2022,* *https://www.apple.com/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/*

Es irónico que los autores del Citizen Lab, que publicaron un informe denominado «CatalanGate», que sugiere que el Gobierno de España está llevando a cabo una vigilancia ilegal «ilimitada, innecesaria y desproporcionada» de la sociedad civil catalana, basada en análisis no reproducibles y datos no verificables recopilados por partidos y activistas partidarios del secesionismo, acusen a un investigador académico con un historial acreditado de publicaciones revisadas por pares[412] que estudian la conexión entre populismo y desinformación y que ha realizado una investigación independiente desde abril de ser un «teórico de la conspiración».[413] Este intento de silenciar una voz crítica también es problemático, dado que muchos de los que han presentado su testimonio sobre Cataluña en la Comisión PEGA eran o supuestas víctimas, o miembros de Citizen Lab, o tenían lazos con este instituto de investigación canadiense, o habían defendido a nacionalistas catalanes públicamente.[414]

Es importante recordar que más de 100 académicos consolidados,[415] comparten muchas de las preocupaciones relativas al estudio CatalanGate recopilado en esta revisión crítica, y que pidieron a la Universidad de Toronto que iniciara una investigación independiente sobre la mala conducta en la investigación del informe. El veto de este testimonio a petición de un grupo organizado con intereses propios sienta un precedente muy peligroso para el Parlamento Europeo y choca con el mandato de la Comisión de Investigación PEGA, que pretende «garantizar que todos los hechos se den a conocer públicamente», como declaró su presidente, Jeroen Lenaers.[416]

412/ *ResearchGate. Jose Javier Olivas Osuna, https://www.researchgate.net/profile/Jose-Javier-Olivas-Osuna*

413/ *Carta a la Universidad de Toronto de 5 de julio de 2022, https://paginadelforodeprofesores.files.wordpress.com/2022/07/letter-to-university-of-toronto-by-foro-de-profesores-5-july-2022-re-catalangate-report.pdf*

414/ *Por ejemplo, el Sr. David Kaye ya había sido contactado por ERC para participar en la campaña de comunicación que el movimiento de independencia puso en marcha en julio de 2020, acusando al Gobierno español de espionaje, incluso antes de los análisis forenses de los dispositivos. Roger Torrent (2021). Pegasus, página 152. También pide que se retiren los cargos de rebelión y se refiere a los dirigentes catalanes en prisión como "presos políticos". Facebook. Carles Puigdemont i Casamajo https://www.facebook.com/watch/?v=561833904536956*

*https://exteriors.gencat.cat/en/ambits-dactuacio/afers_exteriors/delegacions_govern/ue/agenda/act_220713_pegasus*.

415/ *Carta a la Universidad de Toronto, 20 de mayo de 2022, https://paginadelforodeprofesores.files.wordpress.com/2022/05/letter-to-uoft-recommending-independent-investigation-citizen*

416/ *EU Debates. Eudeabates.tv. Youtube. EU Parliament PEGA Committee investigates the use of Pegasus and other spyware. 21 de septiembre de 2022, https://www.youtube.com/watch?v=LciskOzRD4Y*

# 16

# Conclusiones

El supuesto estatus o la reputación no son suficientes en la investigación académica. Los análisis deben ser transparentes, estar debidamente documentados y someterse a una revisión *inter pares* independiente: el informe CatalanGate no cumple con esos elementos, ya que se produjeron todo tipo de irregularidades y conflictos de intereses. Un «guardián de la ciberseguridad», respetado en algún momento, puede estar actuando de manera parcial y poco rigurosa para ayudar a las grandes empresas tecnológicas y a partidos políticos separatistas a presentar demandas legales.

Citizen Lab hace referencia a su prestigio y reputación para disipar críticas bien documentadas y compensar la falta de transparencia en su investigación. Esta opacidad afecta no solo a los datos y muestras de infección, sino también a información que no constituye ningún peligro para la intimidad de los participantes, como cuándo, cómo, dónde y quién realizó los análisis forenses. La reputación por sí sola no debe considerarse una justificación válida para los métodos opacos de investigación. Más aún teniendo en cuenta que Citizen Lab es un actor muy influyente en el ámbito de la ciberseguridad, cuya labor se utiliza como base probatoria en numerosas investigaciones parlamentarias y judiciales y es reproducida por medios de comunicación internacionales que repercuten en la opinión pública.

Las pruebas aportadas por el informe CatalanGate son claramente insuficientes para formular acusaciones específicas, como las que se dirigen contra el Gobierno español. No hay motivos suficientes para afirmar que España ha participado en un espionaje ilegal, ilimitado, innecesario o desproporcionado de políticos y activistas catalanes, como sugiere Citizen Lab.

Este informe parece ser un elemento clave de una campaña de propaganda política cuyo objetivo es presentar una amplia red de políticos y activistas como «víctimas» de las fuerzas de seguridad españolas. Algunas de estas «víctimas» estaban supuestamente implicadas en delitos muy graves que buscaban crear una insurrección civil para lograr la secesión de Cataluña. Las fechas de publicación del informe de Citizen Lab en abril de 2022, así como de los anuncios anteriores a julio de 2020, parecen coincidir perfectamente, ayudando a estos activistas y políticos en su intento de ocultar el efecto negativo de las revelaciones relativas a la colaboración con Rusia, la corrupción y la coordinación de grupos violentos para tomar el control del territorio. La investigación se presentó como una forma de deslegitimar las instituciones españolas, incluidos sus gobernantes, el poder judicial y las fuerzas de seguridad.

Dada la falta de rigor científico y la gravedad de las cuestiones metodológicas y éticas señaladas en el presente documento, se recomienda una investigación independiente de los procesos seguidos en la investigación de Citizen Lab. Se trata de garantizar que los posibles errores o malas prácticas no tengan efectos negativos no deseados en terceros ni menoscaben la reputación de la Universidad de Toronto.

Los tribunales de justicia y los comités de investigación, como los del Parlamento Europeo y el Parlamento catalán, deben solicitar a Citizen Lab o a las presuntas víctimas los dispositivos y los datos recogidos en la investigación catalana, de modo que puedan ser verificados de forma independiente por expertos forenses sin afiliación previa ni vínculos institucionales con el instituto de investigación canadiense. Estos expertos independientes deben encargarse de la realización de los análisis y de la evaluación de la validez y veracidad de los resultados. Este análisis también podría servir para descartar la manipulación masiva de pruebas y la fabricación de resultados positivos aprovechando la ausencia de una cadena de custodia de las pruebas.

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 las organizaciones democráticas españolas merece una mayor atención. 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 institución de investigación que puede afirmar legítimamente ser una de las mejores del mundo. Las pruebas aportadas en esta revisión ilustran la complejidad y la variedad de agentes e instituciones que pueden instrumentalizarse en campañas y tácticas de desinformación política modernas (Benkler *et al.* 2018; Krafft of Donovan 2020; Llorca-Asensi *et al.* 2021; Curiel *et al.* 2022).[417]

Quienes han estado supervisando préviamente a los gigantes tecnológicos sobre su transparencia y sus potenciales violaciones del derecho a la intimidad no deberían convertirse en sus agentes y trabajar para desviar el escrutinio público de estas empresas y sus responsabilidades *vis a vis* los ciudadanos europeos. Los gobiernos y, por supuesto, las empresas de programas espía deben rendir cuentas públicamente y deben regularse mejor. Sin embargo, este objetivo no siempre justifica los medios. Este es el caso, en particular, en el contexto del mundo académico en una época en la que la desinformación amenaza la democrácia cada vez más. Si los académicos terminan incumpliendo sus normas y convenciones deontológicas, la ciencia y la educación pueden verse desacreditadas. Tanto las universidades como los periodistas, así como los representantes públicos, deben ejercer sus competencias para garantizar la veracidad de la información y reprimir los abusos de autoridad y la manipulación por parte de grupos con intereses políticos y económicos personales. Hoy en día, cuando las técnicas de desinformación son cada vez más sofisticadas y difíciles de rebatir, esto debe ser una prioridad.

417/

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

17

# Agradecimiento

Este análisis crítico recoge la información recopilada entre abril de 2022 y enero de 2023 en relación con la investigación y el informe de CatalanGate. Gran parte de la información recopilada se ha hecho pública anteriormente en Twitter y en algunos documentos de opinión escritos por el autor de esta revisión. Varios académicos y periodistas ayudaron a través del proceso de recopilación de datos. En noviembre de 2022, el eurodiputado Jordi Cañas se puso en contacto con el autor y encargó la redacción de un informe que recopilara y organizase toda la información sobre el caso anteriormente compartido que pudiera ser útil para las deliberaciones sobre el caso de espionaje en España.

# Acerca del autor

José Javier Olivas Osuna es el investigador principal del Proyecto Interdisciplinario Comparativo sobre el Populismo y el secesionismo (ICPPS) y de «Populism and Borders: a Supply and Demand-Side Comparative Analysis of Discourses and Attitudes» en el Departamento de Ciencia Política y de la Administración de la Universidad Nacional de Educación a Distancia (UNED) de Madrid. También es asociado a la investigación en el LSE IDEAS y ha dirigido trabajos de consultoría sobre políticas públicas para la UE y otras organizaciones internacionales. Posee un doctorado en Gobierno (LSE) y un MSc en Política Pública y Administración (LSE). Previamente, obtuvo los títulos universitarios en Economía y Empresa (ETEA, Universidad de Córdoba), Investigación de Mercado (ETEA) y Estudios Europeos (EDHEC, Lille).

José Javier coordinó el proyecto de investigación «Debatiendo Brexit a nivel local: un estudio comparativo de métodos mixtos» (con Mary Kaldor) y varios proyectos y actividades docentes de innovación en la LSE. También codirigió el proyecto «Democracia y actitudes populistas en Andalucía: un análisis comparado multidisciplinar» (con Manuel Arias Maldonado) y ha colaborado con los proyectos Psycorona, Varieties of Democracy (V-Dem) y el consorcio CIVICA «Movilización local contra la UE. Dimensiones territoriales del euroescepticismo populista». Sus intereses de investigación incluyen también la política pública, las fronteras, la comunicación política, la desinformación, las respuestas a la COVID-19 y la democratización. Ha publicado en revistas como *Gobernanza, Política y Sociedad, European Journal of Political Research y European Journal of Communication*, y es el autor de la monografía «Iberian Military Politics Controlling the Armed Forces during Dictatorship and Democratisation (Palgrave)». José Javier habla español (nativo), inglés, francés, portugués e italiano. Escribe documentos de orientación para organizaciones internacionales y suele ser entrevistado en medios de comunicación, también escribe publicaciones en blogs académicos y es activo en Twitter: @josejolivas

# Bibliografía

Abela, K. J., Angeles, D. K., Alas, J. R. D., Tolentino, R. J., & Gomez, M. A. (2013). An automated malware detection system for android using behavior-based analysis AMDA. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2(2), 1-11

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

Al-Maskati, M., Marczak, B., Anstis, S., & Deibert, R. (2022) Peace through Pegasus Jordanian Human Rights Defenders and Journalists Hacked with Pegasus Spyware, Citizen Lab, 5 April 2022, https://citizenlab.ca/2022/04/peace-through-pegasus-jordanian-human-rights-defenders-and-journalists-hacked-with-pegasus-spyware/

Arshad, H., Jantan, A. B., & Abiodun, O. I. (2018). Digital forensics: review of issues in scientific validation of digital evidence. Journal of Information Processing Systems, 14(2), 346-376
Ayers, R., Brothers, S. & Jansen, W. (2014). Guidelines on Mobile Device Forensics. NIST Special Publication 800-101. Revision 1. http://dx.doi.org/10.6028/NIST.SP.800-101r1

Ballard, B., Cutinha, A., & Parsons, C. (2021). Pandemic Privacy A Preliminary Analysis of Collection Technologies, Data Collection Laws, and Legislative Reform during COVID-19. Citizen Lab, 28 September 2021, https://citizenlab.ca/2021/09/pandemic-privacy-collection-technologies-data-collection-laws-and-legislative-reform-during-covid-19/

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

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

Marczak, B., Scott-Railton, J., Senft, A., Razzak, B. A., & Deibert, R. (2018). The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil, The Citizen Lab (Oct. 1, 2018), https://tinyurl.com/y9yyhaz3

Cardenal, J. P.(2020). La telaraña. La trama exterior del procés. Barcelona: Editorial Ariel

CEPA (2021). Catalonia: Where There's Trouble There's Russia. 27 September 2021, https://cepa.org/article/catalonia-where-theres-trouble-theres-russia/

Coppedge, M., Gerring, J. & Ziblatt D. (2021). V-Dem [Country–Year/Country–Date] Dataset v11.1. Varieties of Democracy (V-Dem) Project. https://doi.org/10.23696/vdemds21.

Cuixart, J. (2019). Ho tornarem a fer. Quan la injustícia és la llei, la desobediència civil és un dret. Barcelona: ARA Llibres

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

Dalek, J., Dumlao, N., Kenyon, M., Poetranto, I., Senft, A., Wesley, C., Filastò, A., Xynou, M., & Bishop, A. (2021). No Access LGBTIQ Website Censorship in Six Countries. Citizen Lab, 31 August 2021. https://citizenlab.ca/2021/08/no-access-lgbtiq-website-censorship-in-six-countries/

Deibert, R. (2016). My conversations with Edward Snowden. 3 April 2016. https://deibert.citizenlab.ca/2016/04/chatting-with-snowden/

Deibert, R. (2017) The DHS/FBI Report on Russian Hacking was a Predictable Failure, Just Security, 4 January 2017, https://www.justsecurity.org/35989/dhsfbi-report-russian-hacking-predictable-failure/

Deibert, R. (2020). Reset: Reclaiming the Internet for Civil Society. The CBC Lectures. House of Anasi Press. https://houseofanansi.com/products/reset

Deibert, R. (2022). CatalanGate Report Correcting a Case. 22 December 2022, https://citizenlab.ca/2022/12/catalangate-report-correcting-a-case/

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.

Ponsatí Obiols, C. (2022) European Parliament Debates. Whitewashing of the anti-European extreme right in the EU (topic debate) https://www.europarl.europa.eu/doceo/document/CRE-9-2022-10-19-INT-3-149-0000_EN.html

Expert Panel on Research Integrity (2010). Honesty, Accountability and Trust: Fostering Research Integrity in Canada. Council of Canadian Academies https://cca-reports.ca/wp-content/uploads/2018/10/ri_report.pdf

Farrow, Ronan (2022). How Democracies Spy on their Citizens. The New Yorker, 25 April 2022 https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens

Guarnieri, C., & Maynier, E. (2021) Mobile Verification Toolkit. Github. https://github.com/mvt-project/mvt

Hernández, G., & C. (2022). The challenge of Catalan secessionism to the European model of the rule of law. Hague Journal on the Rule of Law, 1-29;

Horsman, G. (2019). Tool testing and reliability issues in the field of digital forensics. Digital Investigation, 28, 163-175

Hughes, N., & Karabiyik, U. (2020). Towards reliable digital forensics investigations through measurement science. Wiley Interdisciplinary Reviews: Forensic Science, 2(4), e1367.

Hulcoop, A., Scott-Railton, J., Tanchak, P., Brooks, M., & Deibert, R. (2017). Tainted Leaks Disinformation and Phishing With a Russian Nexus. Citizen Lab 25 May 2017. https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/

Scott-Railton, J., Marczak, B., Guarnieri, C., & Crete-Nishihata, M. (2017), Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links, The Citizen Lab (Feb. 11, 2017), https://tinyurl.com/ya3tgrhr

Junqueras, O. & Rovira, M. (2020), Tornarem a vencer (i com ho farem). Barcelona: ARA Llibres

Kenyon, M. (2020) Citizen Lab and Amnesty International Uncover Spyware Operation Against Indian Human Rights Defenders. Citizen Lab, 15 June 2020 https://citizenlab.ca/2020/06/citizen-lab-amnesty-international-uncover-spyware-operation-against-indian-human-rights-defenders/

Knockel, J. & Ruan, L. (2022). Engrave Condition Apple's Political Censorship Leaves Taiwan, Remains in Hong Kong. Citizen Lab, 22 March 2022, https://citizenlab.ca/2022/03/engrave-condition-apples-political-censorship-leaves-taiwan-remains-in-hong-kong/

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

LeBel, Etienne P., Berger, D., Campbell, L., & Loving, T. J. (2017). Falsifiability is not optional. Journal of Personality and Social Psychology, 113(2), 254–261

Lin, P. (2022). Privacy and Security Analysis of the IATA Travel Pass Android App. Citizen Lab, 13 April 2022, https://citizenlab.ca/2022/04/privacy-and-security-analysis-of-the-iata-travel-pass-android-app/

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

Marczak, B. & Scott-Railton, J. (2016), The Citizen Lab, The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender 5 (Aug. 24, 2016), https://tinyurl.com/y3uvmlev;

Marczak, B., Abdulemam, A., Al-Jizawi, N., Anstis, S., Berdan, K., Scott-Railton, J., & Deibert, R. (2021). From Pearl to Pegasus Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits, Citizen Lab, 24 August 2021, https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/

Marczak, B., Scott-Railton, J., Razzak, B. A., Al-Jizawi, N., Anstis, S., Berdan, K., & Deibert, R. (2021). Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware, Citizen Lab, 16 December 2021, https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

Marczak, B., Scott-Railton, J., Razzak, B. A., Al-Jizawi, N., Anstis, S., Berdan, K., & Deibert, R. (2021), FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild. Citizen Lab, 13 September 2021, https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/

Marczak, B., Scott-Railton, J., Berdan, K., Razzak, B. A., & Deibert, R. (2021). Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus. Citizen Lab, 15 July 2021, https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

Marczak, B., Scott-Railton, J., McKune, S., Razzak, B. A., & Deibert, R. (2018). Hide and Seek:Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Marczak, B., Scott-Railton, J., Anstis, S., & Deibert, R. (2017). Independent Peer Review of Amnesty International's Forensic Methods for Identifying Pegasus Spyware. Citizen Lab. 18 July 2021 https://citizenlab.ca/2021/07/amnesty-peer-review/

Marczak, B., Scott-Railton, J., Anstis, S., Razzak, B. A., & Deibert, R. (2021). Breaking the News: New York Times Journalist Ben Hubbard Hacked with Pegasus after Reporting on Previous Hacking Attempts, Citizen Lab, 24 October 2021, https://citizenlab.ca/2021/10/breaking-news-new-york-times-journalist-ben-hubbard-pegasus/

Martín, Gregorio and Scott, Jonathan Scott (2023) CatalanGate Vectors: An Analysis of WhatsApp's Impact on Citizen Privacy and Amnesty International's MVT- Tool, January 2023, https://www.researchgate.net/ publication/367078083_CATALANGATE_VECTORS_An_ Analysis_of_WhatsApp's_Impact_on_Citizen_Privacy_and_ Amnesty_International's_MVT-_Tool

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

Montasari, R., Hill, R., Carpenter, V., & Hosseinian-Far, A. (2019). The standardised digital forensic investigation process model (SDFIPM). In Blockchain and Clinical Trial (pp. 169-209). Springer, Cham.

Mukasey, M.B., Sedgwick, J.L. & Hagy, D.W. (2008). Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, NCJ 219941, April 2008, U.S. Department of Justice Office of Justice Programs https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

OCCRP (2021). Catalan Separatists Tailored Public Messaging to Avoid Antagonizing Russia: 'You Have to Avoid Navalny For Sure', Organized Crime and Corruption Reporting Project, 3 September 2021,. https://www.occrp.org/en/investigations/catalan-separatists-tailored-public-messaging-to-avoid-antagonizing-russia-you-have-to-avoid-navalny-for-sure

OCCRP (2022). Fueling Secession, Promising Bitcoins: How a Russian Operator Urged Catalonian Leaders to Break With Madrid, Organized Crime and Corruption Reporting Project, https://www.occrp.org/en/investigations/fueling-secession-promising-bitcoins-how-a-russian-operator-urged-catalonian-leaders-to-break-with-madrid

Olivas Osuna, J. J. (2022). Methodological and ethical issues in Citizen Lab's spyware investigation in Catalonia, document publicly available on ResearchGate: https://www.researchgate.net/publication/361140330_Methodological_and_ethical_issues_in_Citizen_Lab's_spyware_investigation_in_Catalonia
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

Pandey, P., Almodaresi, F., Bender, M. A., Ferdman, M., Johnson, R., & Patro, R. (2018). Mantis: a fast, small, and exact large-scale sequence-search index. Cell Systems, 7(2), 201-207.

Poblet, M. (2018). Distributed, privacy-enhancing technologies in the 2017 Catalan referendum on independence: New tactics and models of participatory democracy. First Monday. https://firstmonday.org/ojs/index.php/fm/article/view/9402

Puigdemont, C. (2019). The Catalan Independence Movement Has Proven Its Strength. Now Spain's Government Must Talk to Us. Time. 21 October 2019, https://time.com/5705915/carles-puigdemont-catalan-protest-barcelona/

Puigneró, J. (2020). El 5è poder: La República Digital a les teves mans. La Campana.

Roberts, K. M. (2022). Performing Crisis? Trump, Populism and the GOP in the Age of COVID-19. Government and Opposition, 1-19.

Deibert, R. (2022). The Autocrat in Your iPhone. Foreign Affairs. 12 December 2022. January/February 2023 issue. https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert

Scott, J. B. (2022). Review of Catalangate Amnesty International Validation, 25 November 2022, 10.13140/RG.2.2.10512.28160 https://www.researchgate.net/publication/365743925_Review_of_Catalangate_Amnesty_International_Validation

Scott-Railton, J., Marczak, B., Nigro Herrero, P., Razzak, B.A., Al-Jizawi, N., Solimano, S., & Deibert, R. (2022). Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware, Citizen Lab, 12 January 2022, https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/

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. Citizen Lab, 18 April 2022

Torrent, R. (2021). Pegasus: L'Estat que ens espia. Barcelona: Ara Llibres.

United Nations (2022). 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

University of Toronto (2019) Research Integrity https://research.utoronto.ca/research-integrity/research-integrity

University of Toronto Governing Council (1991) Policy on Ethical Conduct in Research, https://governingcouncil.utoronto.ca/system/files/import-files/ppmar281991i4820.pdf

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). Digital forensics vs. Anti-digital forensics: Techniques, limitations and recommendations. arXiv preprint arXiv:2103.17028.

# Declaraciones y cartas


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 December 2020 https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2020/12/NSO-v.-WhatsApp-Amicus-Brief-Microsoft-et-al.-as-filed.pdf

Citizen Lab (2018) Letter to Lyndon Cantor, CEO from Paliare Roland Barristers, 8 March 2018. https://citizenlab.ca/wp-content/uploads/2018/03/UofT-Sandvine-Letter-to-Lyndon-Cantor-signed-8-March-2018.pdf

Deibert, Ronald (2021) Statement of Ronald J. Deibert. Immigration Division. Immigration and Refugee Board of Canada, ID File No: 0018-C1-00135-01. UCI: 11-0952-9374. Statement in the context of Chelsea Manning's inadmissibility proceeding. Revised 16 October 2021. https://policycommons.net/artifacts/1961557/statement-of-ronald-j-deibert/2713322/

Deibert, Ronald (2022), Formal letter responding to questions from six Renew Europe MEPs on 13 May 2022 MEPs (letter sent by Mrs Lorraine Ferris to Mr Jordi Cañas published on Citizen Lab's website https://deibert.citizenlab.ca/wp-content/uploads/2022/05/2022.05.13-L-Ferris-to-J-Canas.pdf).

Formal complaint presented by Mr Gonzalo Boye in Madrid Court on 3 May 2022, https://files.mediaset.es/file/10002/2022/05/03/Querella_Pegasus_-Gonzalo_BOYE-_-1-_-2_5367.pdf

Letter to the University of Toronto by 16 international researchers, 20 May 2022, https://paginadelforodeprofesores.files.wordpress.com/2022/05/letter-to-uoft-recommending-independent-investigation-citizen

Letter to the University of Toronto by Foro de Professores, 5 July 2022, https://paginadelforodeprofesores.files.wordpress.com/2022/07/letter-to-university-of-toronto-by-foro-de-profesores-5-july-2022-re-catalangate-report.pdf

University of Toronto. Annex to Letter in response to FIPPA Request #22-0052, 21 September 2022

University of Toronto. Letter in response to FIPPA Request #22-0052, 22 August 2022

# Vídeos


Access Now. Fireside Chat: Ron Deibert, Edward Snowden & Amie Stepanovich - The Hub. Youtube. 1 April 2016, https://www.youtube.com/watch?v=yGDqXokPGiE

Anonymous Oficial. Nobody Knows About This "Prepare Yourself". Youtube. 24 February 2021, https://www.youtube.com/watch?v=d40oHhECx_I

Assemblea. Catalan Gate, 26 April 2022, https://www.youtube.com/watch?v=GGUr7Guk300

Assemblea. Elisenda Paluzie #CatalanGate, 29 April 2022, https://www.youtube.com/watch?v=G5TDEFBMYU0

Assemblea. Jordi Sànchez #CatalanGate. 26 April 2022, https://youtu.be/9crBYexH6Ew

Assemblea. Sonia Urpí #CatalanGate. Youtube. 26 April 2022. https://www.youtube.com/watch?v=jH6Q1ZFLUm0

Canòdrom Ateneu d'Innovació Digital i Democràtica. A l'ombra de Pegasus | Drets civils en l'era de la vigilancia. 3 November 2022. Youtube. https://www.youtube.com/watch?app=desktop&v=OcFBZBlWttY&feature=emb_imp_woyt

Carles Puigdemont I Casamajo (capture from Digital Talk) https://www.facebook.com/watch/?v=561833904536956

CCMA.cat. TV3. No pot ser! Elies Campo: el català que va fugir de WhatsApp quan va conèixer Facebook per dins. 14 April 2019, https://www.ccma.cat/tv3/alacarta/no-pot-ser/elies-campo-el-catala-que-va-fugir-de-whatsapp-quan-va-coneixer-facebook-per-dins/video/5844428/

CCMA.cat. TV3. Pegasus, l'espia a la butxaca. 16 October 2022, https://www.ccma.cat/tv3/alacarta/30-minuts/pegasus-lespia-a-la-butxaca/video/6180772/

CCMA.Cat. TV3. Preguntes Freqüentes. El Catalangate amb John Scott-Railton i Elies Campo, Lang Lang i Noemí Casquet, 23 April 2022; https://www.ccma.cat/tv3/alacarta/preguntes-frequents/el-catalangate-amb-john-scott-railton-i-elies-campo-lang-lang-i-noemi-casquet/video/6155478/

CCMA.cat. TV3. Pregunts frequents. Gonzalo Boye: "Hem sigut espiats i hi ha proves". 30 April 2022. https://www.ccma.cat/tv3/alacarta/preguntes-frequents/gonzalo-boye-hem-sigut-espiats-i-hi-ha-proves/video/6156598/

CCMA.cat. TV3. Pregunts frequents. Jordi Baylina: "He assumit que visc amb un mòbil espiat". 30 April 2020, https://www.ccma.cat/tv3/alacarta/preguntes-frequents/jordi-baylina-he-assumit-que-visc-amb-un-mobil-espiat/video/6156617/

Club Suisse de la Presse. Human Rights and New Technologies. Illegal surveillance as a global challenge to democracy, human rights and its impact on civil society: the Catalangate case. 30 June 2022, https://pressclub.ch/human-rights-and-new-technologies-illegal-surveillance-as-a-global-challenge-to-democracy-human-rights-and-its-impact-on-civil-society-the-catalangate-case/

El Periódico. VÍDEO | Víctor Terradellas, ante el juez: "Puigdemont no declinó la oferta de los rusos. Solo dijo: 'seguid hablando'", 20 May 2022, https://www.elperiodico.com/es/politica/20220520/victor-terradellas-declaracion-integra-trama-rusa-proces-video-13682154

EU Debates. Eudeabates.tv. Youtube. EU Parliament PEGA Committee investigates the use of Pegasus and other spyware, 21 September 2022, https://www.youtube.com/watch?v=LciskOzRD4Y

European Parliament, Multimedia Centre, Committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, 28 November 2022, https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20221129-0900-COMMITTEE-PEGA

European Parliament. Multimedia Centre. Committee of Inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, 6 October 2022, https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20221006-0900-COMMITTEE-PEGA

Expert testimony of Mr Gregorio Martín Computation Professor (retired) at University of Valencia European Parliament, Multimedia Centre, Committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, 28 November 2022, https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20221129-0900-COMMITTEE-PEGA

FES Acatlán. UNAM. Facebook. Mesa redonda sobre el caso de espionaje masivo #CatalanGate, 27 May 2022, https://www.facebook.com/unamacatlan/videos/517790730094535

France TV. La Fabrique du Mensonge Au cœur de la propagande russe, 11 December 2022, https://www.france.tv/france-5/la-fabrique-du-mensonge/la-fabrique-du-mensonge-saison-3/4367680-au-coeur-de-la-propagande-russe.html

Hack Patrol, Getting Pegasus (NSO) False Positive. Vimeo, 7 April 2022, https://vimeo.com/696991504

La República Digital Catalana. Youtube, 21 May 2020, https://www.youtube.com/watch?v=Z6uQZDP0C1Q

La República. Cuixart: "Ho tornarem a fer i no en tinc cap dubte, perquè l'única lluita que es perd és la que s'abandona." 11 July 2020, https://www.larepublica.cat/noticies/video-cuixart-ho-tornarem-a-fer-i-no-en-tinc-cap-dubte-perque-lunica-lluita-que-es-perd-es-la-que-sabandona/

La Vanguardia. Los audios de la operación Vóljov, Youtube 4 November 2020, https://www.youtube.com/watch?v=gQ9TlPnZ-xU

LDPR-TV. Митинг у Посольства Испании. Жириновский живьем от. Youtube, 10 November, 2017. https://www.youtube.com/watch?v=rFNyjBPoyno

PACE public hearing: Pegasus and similar spyware and secret state surveillance. Youtube, 12 December 2022. https://www.youtube.com/watch?v=zZft_l0cWJs

Studentersamfundet i Trondhjem. Meet Snowden. Youtube, 11 March 2018, https://www.youtube.com/watch?v=nQ83xLdOtCQ

The Wire. Youtube. Your Smartphone Is Worse Than A Spy in Your Pocket: Edward Snowden. 22 July 2021, https://www.youtube.com/watch?v=quj2NG34834

The Yellows Catalonia. The Yellows 21 – Ho ternarem a fer. Youtube, 17 June 2019, https://youtu.be/yqjIyscbi7o

Web3 Foundation. Youtube. Jordi Baylina Presents Building a new Decentralized State at Web3 Summit 2019. Youtube, 20 September 2019, https://www.youtube.com/watch?v=P2L-8ZqZ-7CI&t=1s

# Páginas web


Apple. Newsroom, 22 July 2022, https://www.apple.com/uk/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/

Apple. Newsroom, 23 November 2021, https://www.apple.com/newsroom/pdfs/Apple_v_NSO_Complaint_112321.pdf

Apple. Newsroom. 6 July 2022, https://www.apple.com/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/

CatalanGate Ens Estan Vigilant https://catalangate.cat/

Citizen Lab Publications. https://citizenlab.ca/publications/

Citizen Lab. About. https://citizenlab.ca/about/

Forbidden Stories. About The Pegasus Project. https://forbiddenstories.org/about-the-pegasus-project/

Forbidden Stories. Journalists Under Surveillance. https://forbiddenstories.org/pegasus-journalists-under-surveillance/

Fundacio Nord, https://www.fundacionord.cat/en

Gencat. Blockchain Strategy of Catalonia. June 2019, https://smartcatalonia.gencat.cat/en/projectes/tecnologies/detalls/article/estrategia-blockchain-de-catalunya

GenCat. Catalunya 2022. https://presidencia.gencat.cat/ca/ambits_d_actuacio/catalunya-2022/

GenCat. Impact of Modern Spyware Tools on Fundamental Rights. https://exteriors.gencat.cat/en/ambits-dactuacio/afers_exteriors/delegacions_govern/ue/agenda/act_220713_pegasus

Github AmnestyTech / investigations. Remove a file that creates false positive. 29 July 2021, https://github.com/AmnestyTech/investigations/

Github. Jonathandata1/Pegasus-CatalanGate-False-Positives, 25 November 2022, https://github.com/jonathandata1/Pegasus-CatalanGate-False-Positives

Govern.cat. Sala Premsa. 10 September 2021, https://govern.cat/salapremsa/notes-premsa/413472/vic-subseu-del-centre-blockchain-catalunya

https://www.apple.com/uk/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/

IMDB. Black Code. 2016. https://m.imdb.com/title/tt5937964/

LinkedIn. Elies Campo. https://www.linkedin.com/in/eliescampo
Munk School of Global Affairs & Public Policy Citizen Lab Fund, https://engage.utoronto.ca/site/SpageServer?pagename=donate#/fund/847

Òmnium. CatalanGate: Democràcia Vigilada. Fes un Donatiu! https://catalangate.Òmnium.cat/

University of Toronto. Framework to Address Allegations of Research Misconduct of the University of Toronto (2013) https://research.utoronto.ca/media/48/download

University of Toronto. Research Integrity. https://research.utoronto.ca/research-integrity/research-integrity

University of Toronto. Snowden lawyer discusses need for Citizen Lab with director Ron Deibert. 4 February 2016, https://politics.utoronto.ca/2016/02/snowden-lawyer-discusses-need-for-citizen-lab-with-director-ron-deibert/

# Prensa (incluida online)

20 Minutos
ABC
ARA
The Asian Banker
BBC News
Catalan News
CoinDesk
Confilegal
CoSalud.es
CountingStars
Crónica Global
CTECH
Daily Mail
El Confidencial
El Español
El Independiente
El Mundo
El Nacional.cat
El País
El Periódico
El Periódico de España (EPE)
El Punt Avui
El Triangle
ElDiario.es
ElEconomista.es
ElMón
Euractiv
Euronews
Europa Press
France 24
Indian Express
La Vanguardia
La Voz de Galicia
Le Monde
New Straits Times
Newsclick
NIUS
Political Capital
Político
Público
Reuters
RTVE
Techtarget
The Canadian News
The Guardian
The New York Times
The Objective
The Sydney Mording Herald
The Times
The Times of India
The Washington Post
TV3 Noticies
Vilaweb
VozPopuli
Washington Post
Wired

JORDI CAÑAS

Jordi Cañas Pérez,
Diputado de Ciudadanos
al Parlamento Europeo.

B-1047 Bruselas — BRANDT 05M073
(+ 32) 2 28-45357
jordi.canas@ep.europa.eu
www.europarl.europa.eu

Estudio elaborado para Jordi Cañas Pérez
por José Javier Olivas Osuna.

Bold

Dirección de Arte y Diseño
www.bold.bz

Bruselas, Febrer de 2023.

Traducción del informe en inglés con
**ISBN: 978-84-09-44360-4**

Se permita la difusión y reproducción parcial de esta publicación citando título y autor de la obra.

La certificación FSC® garantiza que esta pública está impresa en materiales procedentes de Bosques donde se respetarán los requisitos médicos, sociales y económicos.

*En abril de 2022 el laboratorio CitizenLab publicó un informe denominado «CatalanGate: Extensive mercenary spyware operation against Catalans using Pegasus and Candiru» sobre el supuesto uso de estos programas maliciosos para infectar los teléfonos de al menos 65 políticos, abogados y miembros de organizaciones del entorno separatista catalán.*

*Mientras el separatismo catalán, en una campaña perfectamente orquestada, utilizaba políticamente este informe para acusar a España de espiar a ciudadanos por motivos ideológicos, algunos académicos denunciaron públicamente que la investigación de Citizen Lab contenía diversas anomalías que cuestionaban que dicho informe o sus autores pudieran ser considerados como fuentes periciales neutrales.*

*Durante los trabajos de la Comisión PEGA del Parlamento Europeo, creada para determinar la vulneración de derechos fundamentales por el uso de este spyware por gobiernos o corporaciones, Citizen Lab consiguió vetar la presencia en la sesión dedicada a España de José Javier Olivas, uno de los académicos que cuestionaban el informe «CatalanGate».*

*Al aceptar cancelaciones, censuras y vetos de quienes, por rigor académico y metodología, criticaban o cuestionaban fuentes utilizadas para conformar el informe final, se enviaba un inquietante mensaje de falta de imparcialidad, pluralidad y contraste de argumentos e ideas, que podría amenazar la credibilidad de las conclusiones de los trabajos de la Comisión.*

*Es por ello, y con la determinación de combatir la censura, los vetos y cancelaciones en la sede de la democracia europea, que publico esta revisión crítica del informe «CatalanGate» de Citizen Lab elaborado por el profesor, académico e investigador José Javier Olivas.*

*Que este estudio contribuya a evitar confundir sospechas, conjeturas o especulaciones con certezas, sirva para aportar argumentos al debate público y contribuya a fundamentar una opinión veraz sobre la cual poder tomar las decisiones adecuadas para defender los derechos y libertades de los ciudadanos europeos sin sacrificar nuestros valores y principios.*

View publication stats