

Spyware in Europa e caso Paragon, c'è una nuova commissione d'inchiesta (informale) contro l'abuso

 wired.it/article/spyware-in-europa-caso-paragon

Rosita Rijtano

20 gennaio 2024



Fermare l'abuso di **spyware** in Europa e un appello diretto alle vittime: **denunciate**.

Sono queste le prime richieste del nuovo intergruppo del Parlamento europeo dedicato ai **software spia**, che sarà presentato il 21 gennaio a Strasburgo. Una "commissione d'inchiesta informale" contro gli abusi, la definisce **Sandro Ruotolo**, europarlamentare del gruppo Alleanza Progressista dei Socialisti e dei Democratici (eletto nelle fila del Partito democratico) e promotore dell'iniziativa, che sarà affiancato da **Saskia Bricmont** (Verdi/Alleanza libera europea), **Krzysztof Brejza** (Partito popolare europeo) e **Veronika Cifrová Ostrihoňová** (Renew).

Un tema diventato urgente in Italia dopo il **caso Paragon**, l'azienda israeliana che ha sviluppato *Graphite*, uno spyware sfruttato anche dalla nostra intelligence. Sono stati **decine gli utenti italiani allertati da Meta e Apple** perché si trovavano nel mirino di un software spia, tanti ancora quelli che non ne sono a conoscenza. Tra loro, anche **giornalisti e attivisti**. *"È inaccettabile che il governo si rifiuti di fare chiarezza"*, dice Ruotolo a *Wired*.

Il precedente della commissione d'inchiesta Pega

Non è la prima volta che il Parlamento europeo si occupa di spyware, programmi malevoli in grado di prendere il **controllo di un dispositivo**, nei casi più sofisticati sfruttando le cosiddette vulnerabilità **zero click**, cioè che non prevedono alcun ruolo attivo da parte della vittima.

Strumenti che le aziende produttrici, [tra cui molte italiane](#), dichiarano di vendere solo ad apparati statali per contrastare criminalità e terrorismo. Negli anni, però, sono stati documentati ripetuti abusi. Un problema diventato chiaro anche in Europa nel 2021, grazie a un'indagine transnazionale condotta da 17 testate giornalistiche, coordinate dal collettivo internazionale di giornaliste e giornalisti [Forbidden Stories](#) e supportate dal team tecnico della ong *Amnesty International*. Lavoro che ha individuato [tracce di Pegasus](#) – spyware di un'altra impresa israeliana ([Nso Group](#)) – sui **dispositivi di giornalisti, attivisti, avvocati, politici e giudici** in Polonia, Spagna, Grecia e Ungheria.

Una rivelazione senza precedenti nel perimetro dell'Unione, che ha dato input a una commissione d'inchiesta europarlamentare chiamata Pega. Si è conclusa a giugno 2023 con una serie di raccomandazioni rivolte a Consiglio e Commissione europei, che puntavano a **limitare l'uso statale degli spyware in Europa a “casi eccezionali e specifici”**, condannandone l'impiego per *"monitorare, ricattare, intimidire, manipolare e screditare l'opposizione, i critici e la società civile, eliminare il controllo democratico e la libertà di stampa, manipolare le elezioni e minare lo Stato di diritto"*. *"Il commercio e l'uso degli spyware devono essere rigorosamente regolamentati"*, si legge nel documento.

Software spia, una minaccia troppo sottovalutata

Tre anni dopo, però, nulla è cambiato. La [trasparenza promessa si è rivelata un bluff](#). *"I ripetuti scandali indicano un fenomeno esteso: una rete di sorveglianza politica, commerciale e militare che attraversa l'Europa e mina la libertà di stampa e i diritti fondamentali"*, afferma Ruotolo, che aggiunge: ***"Lo spionaggio illegale è proprio dei regimi ed è segno di una profonda regressione democratica"***. Da qui la scelta di creare un intergruppo parlamentare: *"Con i nuovi equilibri politici, era l'unica strada possibile* – precisa l'eurodeputato –. *"Il Partito popolare europeo, oggi partito di maggioranza relativa, non avrebbe mai consentito l'istituzione di una nuova commissione d'inchiesta"*.

La prima richiesta formale del gruppo, però, sarà proprio quella di **dare seguito alle raccomandazioni della Pega**. Ma l'obiettivo è anche politico e culturale: *"Bisogna far crescere la consapevolezza della minaccia rappresentata dagli spyware"*, prosegue Ruotolo. *"Ecco perché è fondamentale denunciare. Chi ha ricevuto notifiche da Apple e Meta non deve avere paura di testimoniare. Sappiamo che i casi sono molti di più, anche tra i giornalisti. E non mancano quelli italiani"*.

Il punto sul caso Paragon in Italia

Ma cosa sappiamo finora del caso Paragon in Italia? Di certo, nell'ultimo anno decine di utenze italiane sono state avvise da Apple e Meta di essere state bersaglio di un attacco spyware. [Un'indagine del Copasir](#), il comitato parlamentare di controllo sui servizi segreti, ha accertato che **Graphite è stato utilizzato dall'intelligence italiana** per spiare due attivisti dell'ong *Mediterranea Saving Humans*, **Luca Casarini e Giuseppe Caccia**, e **David Yambio**, portavoce di *Refugees in Libya*.

Ma restano irrisolti i casi dei giornalisti **Francesco Cancellato**, direttore di *Fanpage.it*, e di **Ciro Pellegrino**, caporedattore della stessa testata, così come quelli delle altre vittime ([dieci in tutto, le note](#)). Sugli episodi che sono stati denunciati, le procure di Roma e Napoli hanno aperto un'inchiesta.

Mentre il governo ha alzato un muro. Durante la conferenza stampa di inizio anno, la presidente del Consiglio **Giorgia Meloni** ha sostenuto che il Parlamento ha "escluso l'uso di Graphite nei confronti di giornalisti". **Un'informazione fuorviante**: la relazione del Copasir, infatti, risale a giugno 2025 e non ha verificato cos'è successo allo smartphone di **Pellegrino**, su cui le analisi del Citizen Lab – laboratorio sulla sorveglianza dell'università di Toronto – hanno individuato **tracce riconducibili a Paragon**. "I fatti personali non di Cancellato, ma di Giorgia Meloni, sono finiti su tutti i giornali", ha detto poi la premier spostando l'asse del discorso.

Mancano adeguate tutele per giornaliste e giornalisti (e non solo)

Sandro Ruotolo ritiene allarmante che almeno 37 giornalisti siano stati bersaglio di spyware in Europa. In teoria lo **European Media Freedom Act**, il nuovo regolamento europeo sulla libertà dei mezzi d'informazione, dovrebbe rappresentare uno scudo. L'articolo 4 vieta l'uso di questi strumenti contro giornalisti, fonti e *media service provider*, salvo casi eccezionali legati alla sicurezza nazionale e soggetti a controllo giudiziario indipendente. "Ma a quattro mesi dall'entrata in vigore dell'Emfa, **l'Italia non ha ancora un quadro giuridico specifico per prevenire la sorveglianza illegale dei giornalisti**", osserva Ruotolo.

Secondo **Lory Roussey**, fondatrice dell'ong Data Rights, il problema è anche strutturale: "Anche se l'Emfa punta a introdurre garanzie, consente l'uso di spyware a determinate condizioni che possono essere facilmente aggirate. Il paradosso è che oggi l'unico gruppo per cui l'uso dello spyware è esplicitamente legalizzato a livello Ue è proprio quello dei giornalisti", spiega a *Wired*.

Un altro nodo irrisolto riguarda **le notifiche alle vittime**, un diritto sancito dalla sentenza La Quadrature du Net del 2020: una volta cessata la minaccia, **gli Stati Ue dovrebbero informare le persone sorvegliate**. "Un obbligo che finora è stato sempre disatteso", sottolinea Roussey.