CAMERA DEI DEPUTATI SENATO DELLA REPUBBLICA

XIX LEGISLATURA

Doc. **XXXIV**
n. **4**

COMITATO PARLAMENTARE PER LA SICUREZZA DELLA REPUBBLICA

(istituito con legge 3 agosto 2007, n. 124)

(composto dai deputati: *Guerini*, Presidente, *Donzelli*, Vicepresidente, *Rosato*, Segretario, *Pellegrini* e *Angelo Rossi* e dai senatori: *Claudio Borghi, Enrico Borghi, Mieli, Ronzulli* e *Scarpinato*)

RELAZIONE SULL'UTILIZZO DELLO *SPYWARE* « *GRAPHITE* » DA PARTE DEI SERVIZI DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA

(Relatore: deputato Lorenzo GUERINI)

Approvata nella seduta del 4 giugno 2025

Trasmessa alle Presidenze il 5 giugno 2025

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

PAGINA BIANCA

INDICE

PAGINA BIANCA

Introduzione.

Il Comitato ha avviato un approfondimento sull'attività svolta dai servizi di *intelligence* e dall'Agenzia per la cybersicurezza nazionale (ACN) con riferimento alla vicenda relativa ad alcuni soggetti che sarebbero stati spiati attraverso uno *spyware* prodotto dalla società israeliana *Paragon Solutions* [(1)], fin dalla pubblicazione delle prime informazioni, apparse sul sito *Fanpage.it* nella serata di venerdì 31 gennaio 2025, che rilanciava una notizia già pubblicata sul sito del quotidiano britannico *The Guardian* secondo la quale circa un centinaio di soggetti, tra cui anche giornalisti e attivisti politici, sarebbero stati spiati e intercettati attraverso tale *spyware*.

In proposito, giova ricordare che, ai sensi dell'articolo 30, comma 2, della legge 3 agosto 2007, n. 124, l'oggetto del controllo esercitato dal Comitato è quello di « verificare, in modo sistematico e continuativo, che l'attività del Sistema di informazione per la sicurezza si svolga nel rispetto della Costituzione, delle leggi, nell'esclusivo interesse e per la difesa della Repubblica e delle sue istituzioni ». Si rammenta, inoltre, che nello svolgimento della sua attività istruttoria, il Comitato non dispone dei poteri propri delle Commissioni di inchiesta ai sensi dell'articolo 82, secondo comma, della Costituzione.

Ciò premesso, nella seduta del 4 febbraio 2025, a margine di un'audizione del Sottosegretario di Stato alla Presidenza del Consiglio dei Ministri – Autorità delegata per la sicurezza della Repubblica, il Comitato ha convenuto sull'opportunità di trasmettere allo stesso Sottosegretario una richiesta di elementi informativi sulla vicenda. In riscontro a tale richiesta, il 28 febbraio 2025 il Sottosegretario ha inviato dapprima una nota dal contenuto interlocutorio, per poi rispondere analiticamente nell'ambito di un'audizione svoltasi il 25 marzo 2025.

In parallelo, il Comitato ha ritenuto di svolgere una serie di audizioni, sia a livello istituzionale, sia con soggetti privati direttamente coinvolti nella vicenda.

Il Comitato ha inoltre effettuato, ai sensi dell'articolo 31, comma 14, della legge n. 124 del 2007, sopralluoghi presso le sedi di DIS, AISI e AISE, nonché una visita presso la Procura generale della Corte di appello di Roma, nell'ambito dei quali ha potuto svolgere, come sarà specificato successivamente, approfondite verifiche sia a livello documentale sia a livello tecnico-operativo sull'utilizzo dello *spyware Graphite*.

Si precisa che le informazioni contenute nella presente relazione, acquisite dal Comitato nell'ambito dell'attività istruttoria svolta, pur essendo spesso caratterizzate da un elevato livello di sensibilità, non sono soggette ad alcuna classifica di segretezza.

Il Comitato si riserva comunque la possibilità di svolgere ulteriori approfondimenti, anche successivamente alla pubblicazione della presente relazione, su eventuali profili di competenza in relazione alle

(1) Si ricorda che, come riportato da fonti aperte, la società *Paragon Solutions* è stata fondata in Israele da diversi soggetti tra i quali l'ex Primo Ministro, Ehud Barak, e l'ex comandante dell'Unità 8200 – l'unità militare delle forze armate israeliane incaricata dello spionaggio dei segnali elettromagnetici e della guerra cibernetica – Ehud Schneorson. La società è stata, peraltro, interessata da un'operazione di acquisizione da parte di un fondo di investimento americano.

presunte intrusioni in dispositivi mobili rese note da altri due giornalisti nelle ultime settimane.

Attività svolta.

Nel periodo tra il 4 febbraio 2025 e la data di approvazione della presente relazione, il Comitato ha approfondito la vicenda relativa ad alcuni soggetti di cui si è pubblicamente affermato essere stati oggetto di attività di intercettazione attraverso lo *spyware* prodotto dalla società israeliana *Paragon Solutions* nel corso di otto audizioni e di ulteriori dieci sedute dedicate alla discussione tra i componenti della proposta di relazione. Alle sedute svolte presso la sede del Comitato si aggiungono quattro sopralluoghi effettuati, rispettivamente, presso il DIS, l'AISI, l'AISE e la Procura generale presso la Corte di appello di Roma.

In particolare, sono stati auditi: il Direttore dell'Agenzia informazioni e sicurezza esterna (AISE), prefetto Giovanni Caravelli (11 febbraio 2025), il Direttore dell'Agenzia informazioni e sicurezza interna (AISI), dottor Bruno Valensise (18 febbraio 2025), il Direttore generale dell'Agenzia per la cybersicurezza nazionale (ACN), prefetto Bruno Frattasi (4 marzo 2025), il Procuratore generale presso la Corte di appello di Roma, dottor Giuseppe Amato (11 marzo 2025), rappresentanti della società Meta in Italia (18 marzo 2025), il Sottosegretario di Stato alla Presidenza del Consiglio dei Ministri – Autorità delegata per la sicurezza della Repubblica, dottor Alfredo Mantovano (25 marzo 2025), rappresentanti della società *Paragon Solutions* (9 aprile 2025) e rappresentanti del laboratorio *The CitizenLab* dell'Università di Toronto (16 aprile 2025).

Anche alla luce di quanto emerso dalle audizioni, il Comitato ha ritenuto altresì di chiedere ai vertici delle Forze di polizia se avessero acquistato ovvero utilizzato a qualunque titolo ovvero comunque fatto ricorso a *software* prodotti dalla società *Paragon Solutions* per l'espletamento dei propri compiti di istituto, con distinte lettere del 26 febbraio 2025, indirizzate rispettivamente al Comandante generale dell'Arma dei Carabinieri, al Comandante generale della Guardia di Finanza e al Capo della Polizia – Direttore generale della pubblica sicurezza. Il Comitato non ha ritenuto di scrivere analoga lettera al Capo del Dipartimento dell'Amministrazione penitenziaria (DAP), in quanto il Ministro della giustizia, con nota in data 19 febbraio 2025, aveva, di sua iniziativa, precisato al Comitato che tale tecnologia non risultava né acquistata né utilizzata dal DAP o dalle strutture da esso dipendenti, come peraltro riportato anche nell'ambito dello svolgimento di un'interrogazione a risposta immediata alla Camera dei deputati nella seduta dello stesso 19 febbraio 2025.

Con successiva nota del 27 febbraio 2025 il Comitato, in ragione dell'interesse di sicurezza nazionale e comunque per completezza di indagine, pur esulando *stricto sensu* dal controllo sugli organismi di informazione per la sicurezza, ha chiesto al Procuratore nazionale antimafia e antiterrorismo se la struttura da lui diretta ovvero altre Procure della Repubblica avessero acquistato, ovvero utilizzato a qualunque titolo, ovvero fatto ricorso a *software* prodotti dalla società *Paragon Solutions* per l'espletamento dei propri compiti di istituto. In data 4 aprile 2025, è pervenuta al Comitato una risposta, che ha

rappresentato che tutte le Procure che hanno dato riscontro alla richiesta del Procuratore nazionale antimafia e antiterrorismo hanno comunicato di non avere utilizzato il *software* in questione.

Con nota del 3 marzo 2025, il Comandante generale dell'Arma dei Carabinieri ha comunicato che nessun Reparto dipendente dall'Arma ha acquistato, ovvero utilizzato a qualunque titolo, o comunque fatto ricorso allo *spyware* della società *Paragon Solutions*. Analoghe risposte sono pervenute dal Capo della Polizia-Direttore generale della Pubblica sicurezza, con nota del 6 marzo 2025, e dal Comandante generale della Guardia di finanza, con nota del 12 marzo 2025.

Sul punto, peraltro, la stessa società *Paragon Solutions*, rispondendo con una nota scritta ad alcuni quesiti formulati nel corso dell'audizione svoltasi il 9 aprile 2025, ha confermato di avere in Italia rapporti contrattuali esclusivamente con le due Agenzie di *intelligence*, escludendo ogni rapporto con altri soggetti o con le Procure della Repubblica.

L'audizione di carattere generale del Procuratore generale presso la Corte di appello di Roma, tenutasi l'11 marzo 2025, ha consentito poi al Comitato di svolgere una riflessione anche di carattere più ampio sulla disciplina vigente delle intercettazioni preventive condotte dai servizi di informazione per la sicurezza.

Il Comitato ha acquisito dall'Autorità delegata, al fine di un maggiore approfondimento, i dati relativi all'impiego dello strumento delle intercettazioni preventive e un riepilogo delle operazioni svolte con l'impiego delle garanzie funzionali negli ultimi anni. Sono state, inoltre, acquisite dal Comitato note di approfondimento da parte della società Meta, della società *Paragon Solutions* e del laboratorio *The CitizenLab* dell'Università di Toronto, al fine di integrare le rispettive audizioni del 18 marzo 2025, del 9 aprile 2025 e del 16 aprile 2025.

Nella seduta del 23 aprile 2025, il Comitato ha deliberato di richiedere ulteriori elementi istruttori, rispettivamente all'Autorità delegata e al Procuratore generale presso la Corte di appello di Roma.

In particolare, il Comitato ha chiesto, a seguito di quanto emerso nell'audizione del 25 marzo 2025, al Sottosegretario Mantovano di voler comunicare se alcuno tra Luca Casarini, Giuseppe Caccia, Mattia Ferrari e David Yambio sia stato sottoposto a intercettazione, rispettivamente, da parte dell'AISE o dell'AISI, nonché di trasmettere al Comitato ogni elemento di informazione utile al fine di stabilire quale dei predetti soggetti sia stato sottoposto a intercettazione previa autorizzazione del Procuratore generale presso la Corte d'appello di Roma e quale sia stato sottoposto a intercettazione avvalendosi delle autorizzazioni rilasciate ai sensi dell'articolo 18, comma 2, della legge n. 124 del 2007, con l'indicazione, nell'uno e nell'altro caso, dei periodi di ascolto e della tipologia di *software* impiegato, e se, sulla base dell'autorizzazione di condotte previste dalla legge come reato, siano state acquisite telefonate *live*, siano state svolte intercettazioni ambientali, sia stata acquisita messaggistica o altra documentazione, sempre in riferimento ai soggetti citati. Con la medesima nota il Comitato ha richiesto altresì di ricevere una illustrazione delle modalità e della tempistica con le quali si sia proceduto – ai sensi dell'articolo 4-*bis*, comma 4, del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155 – alla distruzione di

tutti i dati relativi all'intercettazione dei soggetti citati, ivi comprese le tracce informatiche presenti in banche dati e *server* nella esclusiva disponibilità dei servizi di informazione per la sicurezza. Infine, è stato richiesto all'Autorità delegata di trasmettere al Comitato copia delle richieste di autorizzazione e delle autorizzazioni rilasciate ai sensi dell'articolo 18, comma 2, della legge n. 124 del 2007, per le condotte previste dalla legge come reato finalizzate a intercettare o acquisire messaggistica, corrispondenza e altra documentazione riferibile a taluno dei soggetti sopra specificati ovvero, in alternativa, di consentire l'accesso del Comitato, ai sensi dell'articolo 31, comma 14, delle legge medesima, presso i competenti uffici per l'esame *in loco* delle citate richieste e autorizzazioni.

Nella nota inviata al Procuratore generale presso la Corte d'appello di Roma il Comitato ha richiesto di voler trasmettere o esibire copia dei decreti autorizzativi e degli eventuali decreti di proroga con i quali siano state autorizzate le intercettazioni preventive nei confronti di Luca Casarini, Giuseppe Caccia, Mattia Ferrari e David Yambio, nonché di voler illustrare la modalità e la tempistica con le quali si sia proceduto – ai sensi dell'articolo 4-*bis*, comma 3, del decreto-legge n. 144 del 2005 convertito, con modificazioni, dalla legge n. 155 del 2005 – alla distruzione della documentazione relativa alle intercettazioni dei soggetti citati, ivi comprese le tracce informatiche presenti in banche dati e *server* nella esclusiva disponibilità dei servizi di informazione per la sicurezza. Il Comitato ha invitato, infine, il Procuratore generale a voler comunicare le sue eventuali riflessioni sul tema specifico della captazione della messaggistica statica, anche alla luce delle considerazioni da lui svolte nel corso della sua audizione presso il Comitato.

Le due richieste sono state riscontrate, rispettivamente, il 2 maggio 2025 dal Sottosegretario Mantovano e il 28 aprile 2025 dal Procuratore generale presso la Corte di appello di Roma.

In particolare, l'Autorità delegata, nel trasmettere una analitica ricostruzione delle vicende richieste dal Comitato, ha manifestato la piena disponibilità del DIS alla consultazione della documentazione archiviata relativa alle richieste di autorizzazione concernenti le persone indicate.

Parimenti, il Procuratore generale ha fornito un esaustivo contributo sulla procedura relativa al rilascio delle autorizzazioni, nonché alle modalità e alla tempistica della distruzione dei documenti e ha condiviso alcune riflessioni, anche *de iure condendo*, sulla questione dell'intercettazione di conversazioni archiviate nei dispositivi mobili. Il Procuratore ha manifestato ampia disponibilità a consentire ai componenti del Comitato di poter consultare tutta la documentazione archiviata presso la Procura generale ai sensi dell'articolo 4-*bis*, comma 3, del decreto-legge n. 144 del 2005, convertito, con modificazioni, dalla legge n. 155 del 2005.

All'esito di tali interlocuzioni, in data 7 maggio 2025 si è svolta una visita presso gli uffici della Procura generale presso la Corte di appello di Roma, nel corso della quale i componenti del Comitato hanno avuto modo di consultare ed esaminare attentamente tutta la documentazione ivi archiviata relativa alle operazioni di intercettazione concluse, concernenti i soggetti oggetto della presente relazione. In particolare, i

componenti hanno avuto la possibilità di leggere l'intera sequenza dei provvedimenti autorizzatori, comprensivi delle varie proroghe, tutte singolarmente e specificamente motivate.

In data 7 maggio 2025 si sono svolti, altresì, previa comunicazione al Presidente del Consiglio dei ministri, ai sensi dell'articolo 31, comma 14, della legge 3 agosto 2007, n. 124, due sopralluoghi, rispettivamente, presso una sede dell'AISI e una sede dell'AISE, nel corso dei quali il Comitato ha potuto approfondire le modalità tecniche di funzionamento dello *spyware Graphite* ed escludere che vi siano stati utilizzi non conformi alla normativa vigente con riferimento ai soggetti presi in considerazione nella presente relazione. Come sarà descritto nel prosieguo della relazione, in particolare i componenti hanno avuto modo di interrogare direttamente il *database* e il registro di *audit* del citato *spyware*.

Il 14 maggio 2025, facendo seguito alla disponibilità comunicata dall'Autorità delegata, il Comitato ha svolto, previa comunicazione al Presidente del Consiglio dei ministri, ai sensi dell'articolo 31, comma 14, della legge n. 124 del 2007, un ulteriore sopralluogo presso la sede del DIS, nel corso del quale i componenti hanno avuto modo di consultare ed esaminare direttamente la documentazione ivi conservata relativa alle richieste di autorizzazione allo svolgimento di intercettazioni e all'utilizzo di garanzie funzionali riguardanti i casi oggetto della presente relazione. Anche in tal caso, il Comitato ha potuto riscontrare il corretto adempimento degli obblighi previsti dalla normativa vigente.

1. La ricostruzione della vicenda.

Sulla base delle audizioni svolte, il Comitato è in grado di fornire una sintetica ricostruzione della dinamica con cui la vicenda relativa all'utilizzo del *spyware Graphite* di *Paragon* si è svolta.

In particolare, è stato preliminarmente chiarito che, a far data dal 17 marzo 2023, l'applicazione *WhatsApp* sarebbe stata esposta involontariamente ad una vulnerabilità *0-day* che avrebbe potuto permettere di aggiungere utenti in una *community*, escludendo il filtro *antispam*. Come sarà specificato successivamente, la società *WhatsApp* ha notato attività sospette nel mese di ottobre 2024 e la vulnerabilità è stata individuata l'11 dicembre 2024 e risolta con l'aggiornamento rilasciato il 17 dicembre del 2024, delimitando in tal modo la finestra nell'ambito della quale si sarebbe potuta verificare l'infezione dei dispositivi mobili con lo *spyware Graphite* della società *Paragon Solutions* attraverso la predetta vulnerabilità.

Con una segnalazione del 15 gennaio 2025, lo studio legale ADVANT NCTM in rappresentanza della società *WhatsApp Ireland Limited*, titolare dei *server* della richiamata applicazione per il mercato europeo, ha comunicato all'Agenzia per la cybersicurezza nazionale – CSIRT Italia il verificarsi di un incidente informatico nel quale erano state coinvolte anche utenze italiane, senza tuttavia riferire il numero di tali utenze e indicando l'azienda *Paragon* come produttrice del *software* attaccante.

L'ACN ha proceduto contestualmente ad informare il Centro nazionale anticrimine informatico per la protezione delle infrastrutture

critiche (CNAIPIC) e la Direzione nazionale antimafia e antiterrorismo (DNAA). Nella giornata del 17 gennaio 2025 l'ACN ha quindi chiesto alla società *WhatsApp Ireland Limited* dettagli sulle utenze italiane coinvolte e sullo *spyware*, che non sono nella disponibilità del Comitato. Nella stessa giornata il citato studio legale rappresentante della società *WhatsApp Ireland Limited* ha fornito ad ACN ulteriori dettagli sulla vulnerabilità e sul numero di utenze europee coinvolte, pari a 61. L'ACN ha provveduto a dare contestuale comunicazione di tali informazioni al CNAIPIC e alla Direzione nazionale antimafia e antiterrorismo, nonché al DIS.

Il successivo 31 gennaio 2025 lo studio legale rappresentante della società *WhatsApp Ireland Limited*, nel rispondere alla citata richiesta dell'ACN del 17 gennaio ha comunicato che le utenze italiane impattate erano nel numero di sette, senza fornirne tuttavia gli estremi, identificando lo *spyware* in *Graphite* prodotto dalla società *Paragon*. Anche tali informazioni sono state contestualmente trasmesse a CNAIPIC, DNAA e DIS.

Il 10 febbraio 2025 ACN ha inviato una richiesta di ulteriori informazioni allo studio legale rappresentante della società *WhatsApp Ireland Limited*, con particolare riferimento alle connesse attività di resilienza. Tale richiesta è stata riscontrata dal richiamato studio legale nella giornata del 13 febbraio 2025, che ha informato ACN che la società *WhatsApp Ireland Limited* aveva notificato in data 31 gennaio 2025 l'incidente anche alle sette utenze italiane. Anche di tale circostanza l'ACN ha informato CNAIPIC, DNAA e DIS.

Il 17 febbraio 2025 lo studio legale rappresentante della società *WhatsApp Ireland Limited* ha trasmesso ad ACN un *report* finale sull'incidente, evidenziando peraltro la potenziale compromissione di altre componenti dei dispositivi mobili interessati e non escludendo pertanto la possibilità di infezione dell'intero dispositivo mobile colpito.

Con successive comunicazioni del 24, 26 e 27 febbraio 2025 l'ACN ha chiesto allo studio legale rappresentante della società *WhatsApp Ireland Limited* informazioni circa una nuova utenza nazionale che sarebbe stata oggetto di compromissione, secondo quando emerso da notizie di stampa. Con una nota del 28 febbraio 2025, la società ha chiarito che i *report* di Meta citati nelle notizie di stampa del 24 febbraio si riferiscono a situazioni differenti da quella in trattazione e che la ulteriore vulnerabilità riscontrata era stata già comunicata al fornitore della libreria *open source* e agli sviluppatori del sistema operativo interessato. Anche di tali interlocuzioni l'ACN ha informato CNAIPIC, DNAA e DIS.

Ai fini della presente relazione risulta altresì utile la lettura incrociata dei richiamati accadimenti con la relativa diffusione sui *media*, che è iniziata solo il 31 gennaio 2025 quando, alle ore 14.55 e poi alle ore 15.21, l'agenzia *Reuters* informava che circa 100 giornalisti ed esponenti della società civile utenti di *WhatsApp* sarebbero stati *target* dello *spyware* dell'azienda israeliana *Paragon Solutions*. Giova evidenziare come, in realtà, dalla metà di gennaio era già emerso che *WhatsApp* aveva identificato 61 utenti potenzialmente compromessi in vari Stati europei, senza chiarezza su quanti fossero effettivamente i giornalisti o altri esponenti della società civile. L'agenzia *Reuters* e successivamente anche un articolo pubblicato sul sito del quotidiano

The Guardian delle 17.11 descrivevano poi la tipologia dell'attacco e il fatto che *WhatsApp* avrebbe informato le vittime dell'intrusione. Sempre il 31 gennaio 2025 alle ore 20.52 il sito *Fanpage.it* pubblicava un articolo secondo il quale, tra gli utenti presi di mira dallo *spyware* israeliano, vi sarebbe stato anche il direttore dello stesso sito, il giornalista Francesco Cancellato, che aveva ricevuto un messaggio dal supporto di *WhatsApp*. Nell'articolo si riportano dichiarazioni di un portavoce della società *WhatsApp* che ha rappresentato di aver interrotto dal dicembre 2024 le attività di uno *spyware*, prodotto dalla società *Paragon*.

L'articolo proseguiva poi riportando notizie già pubblicate dal quotidiano *The Guardian*. Fra i potenziali *target* dello *spyware* nei giorni successivi sarebbero stati indicati dai *media*, oltre a Francesco Cancellato, i cittadini italiani Luca Casarini, Giuseppe Caccia e don Mattia Ferrari, nonché un cittadino sudanese, David Yambio, portavoce dell'ONG *Refugees in Libya*.

Il 6 febbraio 2025 i quotidiani *Haaretz* e *The Guardian* hanno rappresentato come, tramite lo *spyware Graphite*, sarebbero stati infettati apparati di attivisti e di giornalisti e che per tale ragione la società *Paragon Solutions* avrebbe rescisso unilateralmente i rapporti contrattuali con l'Italia.

In relazione al caso di David Yambio, secondo quanto emerso, il 13 novembre 2024, questi sarebbe stato informato con una *email* della società *Apple* del fatto che il suo telefono sarebbe stato compromesso da uno *spyware* non meglio precisato. L'11 febbraio 2025 David Yambio ha reso noto di essere tra le vittime dell'attività di uno *spyware* non meglio precisato. I principali *media* che si sono occupati della vicenda, in particolare l'11 febbraio 2025 il sito *Fanpage.it* e l'agenzia ANSA, nel riportare la notizia hanno messo in correlazione lo *spyware* utilizzato per infettare il dispositivo di Yambio con *Graphite*.

2. Aspetti tecnici relativi all'utilizzo del *software Graphite* prodotto dalla società israeliana *Paragon Solutions*.

Nel corso delle audizioni svolte sono stati, inoltre, chiariti alcuni aspetti tecnici relativi sia alle modalità dell'attacco informatico, sia alle contromisure adottate dalla società Meta, nonché il ruolo di *The CitizenLab*, laboratorio dell'Università di Toronto, la cui attività di ricerca è sostenuta da fondazioni e altri soggetti privati [(2)].

Preliminarmente si ricorda che gli *spyware* sono realizzati da soggetti che spesso, a loro volta, li rivendono, fornendo quindi servizi che possono essere definiti di *cyber* sorveglianza a pagamento. L'utilizzo di tali strumenti pone – allorché si verifichi al di fuori di un contesto di legalità, come quello previsto dalle vigenti disposizioni che in Italia regolano le intercettazioni preventive dei servizi o quelle comunque

(2) In particolare, come riportato dal sito del laboratorio, tra i soggetti finanziatori risultano: *Open Society Foundations*, *The Canada Centre for Global Security Studies*, *Donner Canadian Foundation*, *Ford Foundation*, *Hewlett Foundation*, *HIVOS*, *The Hopewell Fund*, *International Development Research Centre (IDRC)*, *John D. and Catherine T. MacArthur Foundation*, *Oak Foundation*, *Psiphon Inc.*, *The Sigrid Rausing Trust*, *Social Sciences and Humanities Research Council of Canada*, *Walter and Duncan Gordon Foundation*.

disposte dalla magistratura nell'esercizio delle proprie funzioni istituzionali – una serie di problematiche, perché consente l'accesso a tecnologie particolarmente sofisticate ed invasive anche a soggetti non governativi, di fatto mettendo a rischio la *privacy* e la sicurezza dei cittadini e, potenzialmente, anche di soggetti pubblici.

Giova poi precisare che, normalmente, con tali *spyware* l'oggetto della violazione è il singolo dispositivo dell'utente *target*, in quanto i contenuti delle comunicazioni sono normalmente protetti da sistemi di crittografia, cosiddetti *end to end*, che risultano estremamente difficili da violare. Gli *spyware* agiscono quindi nel momento in cui tali dati vengono decrittati sul dispositivo di origine o di destinazione degli stessi. Per tale ragione, nemmeno la società che gestisce i servizi di messaggistica e *VoIP* (*Voice over Internet Protocol*) potrebbe avere accesso ai dati che sono stati eventualmente catturati attraverso lo *spyware*.

Con particolare riferimento allo *spyware Graphite* prodotto dalla società israeliana *Paragon Solutions*, si fa presente che, sulla base delle notizie acquisite dal Comitato, la citata società rende disponibili alla vendita i suoi servizi solo a soggetti pubblici appartenenti a Stati che possano garantire il rispetto dei diritti umani e delle libertà civili, con particolare riferimento ad alcuni parametri relativi al controllo sui clienti e ad un controllo di tipo legale, nonché alle garanzie di tipo tecnologico. Sulla base di tali verifiche, la società *Paragon Solutions*, allo stato, opererebbe con numerosi Stati nel mondo, secondo quanto emerso nel corso dell'attività istruttoria condotta dal Comitato. Giova peraltro precisare che la società impone talune limitazioni operative, escludendo ad esempio la possibilità di intercettare utenze relative ad alcuni Paesi, tra cui non è tuttavia ricompresa l'Italia, le cui utenze possono quindi in astratto essere oggetto di attività intercettiva anche da parte di soggetti stranieri.

Con riferimento alle modalità tecniche con cui si realizza specificamente l'intrusione attraverso lo *spyware Graphite*, è emerso come il soggetto attaccante proceda ad aggiungere l'utenza *target* ad un gruppo *WhatsApp* sfruttando la richiamata vulnerabilità dell'applicazione di messaggistica e ad inviare all'utenza un *file* con estensione *Portable Document Format* (.pdf) senza essere bloccato dai filtri di sicurezza dell'applicazione. Tale *file*, appena recapitato sul dispositivo, genera un'anteprima senza bisogno di alcuna interazione da parte dell'utente, causando l'esecuzione del codice malevolo e quindi installando lo *spyware*.

Pur in assenza di dati dettagliati sulle specifiche caratteristiche dello *spyware Graphite*, si può ritenere che esso, analogamente ad altri *software* dello stesso tipo, sia idoneo a procedere alla raccolta di dati sensibili e alla esecuzione in *background*, cioè senza alcuna evidenza da parte dell'utente. I dati così raccolti sarebbero quindi trasmessi a *server* remoti controllati dal soggetto attaccante.

Secondo quanto rappresentato nel corso delle audizioni, non risulta che, ai sensi della licenza d'uso rilasciata ai servizi italiani, lo *spyware Graphite* possa essere utilizzato per attivare la funzione microfono, per effettuare intercettazioni di comunicazioni tra presenti, per utilizzare la fotocamera, per riprendere situazioni in diretta,

nonché per accedere alla galleria fotografica per esfiltrarne il contenuto.

Secondo i riscontri ottenuti dal Comitato nell'ambito della propria attività istruttoria, emerge come di ogni utilizzo dello *spyware Graphite*, l'operatore, che deve identificarsi con *username* e *password*, lasci una traccia in un *database* o *acquisition log* e nel registro di *audit*. Il *database* è ubicato presso la sede del cliente, raccoglie le informazioni acquisite sul *target* di un'operazione e non risulta accessibile alla società. Nel registro di *audit*, i cui dati sono comunque conservati su *server* presso il cliente, si tiene traccia delle operazioni effettuate e di tutti gli accessi al sistema, ivi inclusi eventuali accessi tecnici per manutenzioni o aggiornamenti da parte della società. Peraltro, i dati acquisiti possono essere cancellati dal *database* direttamente da parte del cliente. Le informazioni presenti nel registro di *audit* invece non possono essere cancellate da parte del cliente. Il Comitato ha specificamente richiesto ed ottenuto, anche nel corso dei sopralluoghi presso le Agenzie svoltisi il 7 maggio 2025, rassicurazioni sul fatto che i dati relativi ai contenuti delle operazioni non sarebbero comunque accessibili alla società *Paragon Solutions*. Parimenti, nel corso delle audizioni, i rappresentanti di *Paragon* hanno sostenuto che la società non avrebbe alcun ruolo nell'utilizzo che il cliente fa del sistema e, in particolare, non avrebbe accesso e non sarebbe a conoscenza dell'identità dei soggetti che vengono presi di mira dai clienti o dei dati che vengono registrati dal suo dispositivo.

Rispetto all'utilizzo di *software* come quello realizzato dalla società *Paragon Solutions* le aziende che forniscono servizi di messaggistica istantanea e telefonia con tecnologia *VoIP* sono impegnate ad adottare contromisure volte a rendere le comunicazioni veicolate tramite queste piattaforme sempre più sicure. Nella presente relazione sono state approfondite, inoltre, le misure adottate dalla società Meta in quanto hanno assunto uno specifico rilievo ai fini della materia oggetto del lavoro di approfondimento del Comitato.

Come emerso anche su alcuni organi di informazione e ulteriormente approfondito nel corso delle audizioni e già ricordato sopra, il *team* di sicurezza di *WhatsApp* ha notato per la prima volta un'attività sospetta nell'ottobre del 2024 e ha conseguentemente avviato le necessarie procedure di verifica e di indagine. Non è stato possibile, allo stato, in mancanza di indicazioni sufficienti, determinare con certezza il momento a partire dal quale sono iniziate le prime intrusioni attraverso il *software* prodotto dalla società *Paragon*, sfruttando l'esistenza del richiamato *bug* nell'applicazione *WhatsApp*. Tale vulnerabilità, che non ha riguardato – sulla base di quanto emerso nel corso delle audizioni – i *server* remoti di *WhatsApp*, è stata poi individuata l'11 dicembre del 2024 ed è stata segnalata al *team* di tecnici competente, che l'ha definitivamente risolta il 17 dicembre 2024, impedendo così ogni ulteriore utilizzo da parte di *Paragon* o dei suoi clienti.

In proposito, risulta confermata la collaborazione tra la società Meta e il laboratorio *The CitizenLab*. In particolare, risulta che, al momento della segnalazione da parte di *The CitizenLab*, Meta stava già conducendo una sua indagine indipendente per accertare le dinamiche

dell'incidente [3]. Pertanto, dalle audizioni svolte, è emerso come i due soggetti abbiano compiuto in parallelo le rispettive attività di verifica.

Con riferimento alle modalità tecniche con le quali sarebbe stato possibile al laboratorio canadese *The CitizenLab* individuare l'infezione informatica, come riportato nel rapporto pubblicato dallo stesso laboratorio il 19 marzo 2025 e confermato nel corso dell'attività conoscitiva, è emerso che sarebbe stato sviluppato un sistema basato su cosiddette « impronte digitali », ovvero tracce informatiche, che rimandano ai certificati dello *spyware*, lasciate in ragione del suo utilizzo nei registri contenuti nei sistemi operativi dei dispositivi interessati. La presenza di tali « impronte » sarebbe stata poi verificata attraverso l'analisi forense di alcuni dispositivi, da parte del citato laboratorio canadese.

La società Meta, in data 31 gennaio 2025, come sopra ricordato, ha contattato direttamente gli utenti potenzialmente interessati tramite una *chat* all'interno dell'applicazione *WhatsApp*. Occorre precisare che l'identità degli utenti non è conosciuta dall'applicazione *WhatsApp*, che, non richiedendo una verifica della loro identità, non può determinare chi siano. In particolare, il testo del messaggio inviato agli utenti risulta il seguente: « Informazioni importanti alla sicurezza. Questo messaggio è di *WhatsApp*. Se desideri verificare questo messaggio, consulta il messaggio di sistema e la spunta blu su questa *chat*. Perché ti stiamo scrivendo ? A dicembre, *WhatsApp* ha bloccato le attività di una società di *spyware* che riteniamo abbia preso di mira il tuo dispositivo. Le nostre indagini indicano che un *file* dannoso potrebbe essere stato inviato all'utente tramite *WhatsApp* e che lo *spyware* potrebbe aver dato accesso ai tuoi dati, compresi i messaggi memorizzati sul tuo dispositivo. Come rimanere al sicuro. Abbiamo apportato delle modifiche per evitare che questo specifico attacco si ripeta. Tuttavia, il sistema operativo del vostro dispositivo potrebbe risultare tuttora compromesso a causa dello *spyware*. Come agire. Si consiglia di cambiare dispositivo, perché anche un *reset* di fabbrica potrebbe non rimuovere lo *spyware*. Se sei un giornalista o un membro della società civile, puoi rivolgerti ai ricercatori in materia di sicurezza del *The CitizenLab* dell'Università di Toronto ». Al citato messaggio segue l'indirizzo *email* del laboratorio canadese e un *link* di collegamento, nonché la disponibilità a rispondere ad eventuali quesiti.

Con riferimento a tale tipo di comunicazioni, si apre una questione relativa alle interazioni tra le autorità di Governo o giudiziarie e le applicazioni di messaggistica o comunicazioni, come *WhatsApp*. Anche tale tema è stato specificamente affrontato nel corso delle audizioni svoltesi.

Con particolare riferimento alla *policy* di Meta illustrata nel corso delle audizioni, risulta che la società fornisca informazioni all'autorità giudiziaria e ad altre autorità di Governo quando necessario e nei termini previsti dalla legge. In particolare, risulta che *WhatsApp* risponda alle richieste legali delle autorità fornendo i dati degli utenti in

(3) In proposito, John Scott Railton, ricercatore *senior* del laboratorio *The CitizenLab*, nel corso dell'audizione del 16 aprile 2025, ha confermato quanto aveva già pubblicato su fonti aperte, dove in data 19 marzo 2025 aveva affermato, in merito all'inizio della ricerca: « Abbiamo ricevuto una soffiata su un singolo pezzo di infrastruttura #*Paragon* e il mio brillante collega @*billmarczak* ha sviluppato una tecnica per rilevare le "impronte digitali" di alcune infrastrutture di *spyware* mercenari (sia rivolte alle vittime che ai clienti) a livello globale. ».

conformità con le leggi vigenti, secondo termini di servizio, politiche e procedure pubblici e pubblicati sulla medesima piattaforma. I risultati di questo lavoro sono peraltro pubblicati due volte all'anno, fornendo informazioni relative alle attività svolte con le Forze di polizia e di sicurezza nel mondo. Il sito contiene, tra l'altro, anche le linee guida operative dedicate alle forze dell'ordine, che indicano la tipologia di informazioni disponibili rilasciabili nel rispetto delle norme vigenti e delle *policy* del gruppo.

In merito alle relazioni tra Meta e *The CitizenLab*, è stato evidenziato peraltro come i due soggetti abbiano intrattenuto in passato anche altri rapporti di collaborazione al fine di approfondire eventuali tecniche di compromissione della riservatezza dei dati e per fornire agli utenti raccomandazioni su come tutelare la loro *privacy* e la loro sicurezza, nonché le modalità con cui operano i fornitori di servizi di *cyber* sorveglianza a pagamento.

3. L'attività dei servizi di informazione per la sicurezza.

3.1. L'impiego dello spyware Graphite *da parte dei servizi di informazione per la sicurezza.*

Nel corso delle audizioni sono stati altresì precisati analiticamente i termini contrattuali relativi all'utilizzo da parte delle Agenzie dello *spyware Graphite* di *Paragon Solutions*, ivi compresi alcuni dettagli economici e operativi che, per ragioni di riservatezza, il Comitato non ritiene di poter rendere pubblici. La presente relazione si limita quindi a indicare gli elementi essenziali dei citati contratti relativi al periodo temporale di utilizzo del *software*.

In particolare, il sistema risulta in uso da parte di AISE a partire dal 23 gennaio 2024 per attività di raccolta informativa nei settori del contrasto a immigrazione clandestina, ricerca latitanti, contrabbando di idrocarburi, controspionaggio, contrasto al terrorismo e criminalità organizzata, nonché per le attività di sicurezza interne all'Agenzia stessa. Il sistema è stato acquistato con contratto sottoscritto il 13 dicembre 2023 ed è stato attivato l'8 febbraio 2024 per il sistema *Android* e il 23 gennaio 2024 per il sistema *iOS*. A partire dal mese di gennaio 2024, lo *spyware Graphite* è stato utilizzato per acquisire dati dinamici, cioè comunicazioni in corso attraverso sistemi cifrati di messaggistica istantanea, relativamente a un numero estremamente limitato di utenze sempre con autorizzazione del Procuratore generale presso la Corte di appello di Roma, ai sensi dell'articolo 4, comma 2, del citato decreto-legge n. 144 del 2005, convertito, con modificazioni, dalla legge n. 155 del 2005, nonché per esfiltrare messaggi di *chat* giacenti nella memoria di dispositivi di *target*, in questo caso con ricorso alle garanzie funzionali, secondo la procedura autorizzativa di cui all'articolo 18, comma 2, della legge n. 124 del 2007.

Risulta al Comitato che l'atto negoziale con cui è stata acquisita la licenza del sistema *Graphite* reca clausole che non consentono, tra l'altro, l'approccio nei confronti di *device* e/o di obiettivi provenienti da determinati Paesi. Inoltre, i termini contrattuali prevedono il divieto di infliggere danno su individui o gruppi di individui semplicemente per religione, sesso, genere, razza, gruppo etnico, orientamento sessuale,

nazionalità, Paese d'origine, opinione o affiliazione politica, età, stato personale, nonché di far uso del sistema nei confronti di giornalisti e attivisti per i diritti umani.

Quanto ad AISI, sulla base delle audizioni svolte, risulta avere avviato la collaborazione con *Paragon* nel 2023. Il contratto in corso sarebbe venuto a scadenza il 7 novembre 2025, con termini negoziali analoghi a quelli riportati nel contratto con AISE. Anche in tal caso, nelle audizioni svolte è emerso che i *target* monitorati mediante l'infezione di dispositivi al fine di intercettazioni telematiche attive, cioè del flusso comunicativo in tempo reale, come tali sottoposte anche all'autorizzazione del Procuratore generale, sarebbero in numero estremamente limitato. Risultano invece poco più numerose, pur essendo in numero contenuto, le acquisizioni telematiche di *chat* residenti nei *device* dei *target*. Tali operazioni sono assoggettate alla disciplina per l'autorizzazione alle condotte previste dalla legge come reato, di cui all'articolo 18, comma 2, della legge n. 124 del 2007. In entrambi i casi, è stato confermato al Comitato che le attività sono state svolte nel rispetto delle autorizzazioni e nei limiti da esse stabiliti, senza peraltro violare i termini indicati nella licenza d'uso.

A seguito del clamore mediatico suscitato dalla vicenda, il 14 febbraio 2025 *Paragon*, AISI e AISE hanno concordemente deciso – secondo quanto chiarito in sede di audizioni al Comitato – di non impiegare, dunque di sospendere temporaneamente, le capacità del *software Graphite* su nuovi *target* rinviando ogni decisione all'esito di approfondimenti da parte del Comitato parlamentare e dell'Agenzia per la cybersicurezza nazionale. Nel corso delle audizioni è stato peraltro specificato che la durata di tale sospensione sarebbe stata determinata in relazione agli esiti dell'approfondimento svolto dal Comitato e oggetto della presente relazione. In occasione dei sopralluoghi effettuati dal Comitato presso le Agenzie, è stato precisato che, successivamente alla sospensione, si è addivenuto alla decisione di rescindere comunque il contratto con *Paragon*.

Si ricorda peraltro che, in sede di svolgimento di una interrogazione a risposta immediata alla Camera dei deputati, in data 12 febbraio 2025, il Governo aveva evidenziato come non fosse stato, a tale data, rescisso alcun contratto della società in questione nei confronti dei servizi di *intelligence*.

3.2. L'attività svolta dai servizi di informazione per la sicurezza.

Con riferimento all'attività dei servizi di informazione per la sicurezza, nell'ambito dei lavori svolti dal Comitato, è emerso come essa si sia svolta nel quadro delle garanzie e dei limiti imposti dalla legge 3 agosto 2007, n. 124.

Analogamente, il Comitato ha avuto modo di verificare, sia nel corso dell'audizione del Procuratore generale presso la Corte d'appello di Roma, sia attraverso l'analisi diretta della documentazione relativa alle operazioni conservata presso gli archivi del DIS e della Procura generale presso la Corte d'appello di Roma, il rispetto delle procedure autorizzative di cui all'articolo 18 della legge n. 124 del 2007, nonché degli obblighi di comunicazione al Comitato, ai sensi dell'articolo 33, comma 4, della medesima legge.

Con specifico riferimento ai soggetti che sono stati indicati dagli organi di stampa come potenzialmente sottoposti ad attività intercettiva da parte dei servizi di informazione per la sicurezza attraverso lo *spyware* prodotto dalla società *Paragon*, alla luce delle audizioni svolte, sono emerse posizioni differenziate tra i diversi soggetti coinvolti.

In particolare, con riferimento a Luca Casarini è stato confermato, sia in sede di audizione che nella documentazione acquisita dal Comitato, che l'attivista è stato, negli anni, oggetto di interesse da parte dei servizi di informazione. In particolare, Casarini risulta tra i soggetti attenzionati nell'ambito di due operazioni condotte dai servizi. La prima, la cui delega è stata rilasciata al termine del 2019 dal Presidente del Consiglio dei ministri *pro tempore*, Giuseppe Conte, si è svolta mediante l'utilizzo di intercettazioni telefoniche, senza il ricorso allo *spyware Graphite*, si è conclusa nel mese di marzo 2020 e ha avuto come scopo l'accertamento della legittimità di un'attività di gestione di flussi migratori. La seconda, di natura più ampia, finalizzata a prevenire la minaccia alla sicurezza nazionale da parte di individui sospettati di svolgere attività di favoreggiamento dell'ingresso di soggetti stranieri nel territorio nazionale, la cui delega è stata rilasciata dal Presidente del Consiglio dei ministri *pro tempore,* Giuseppe Conte, il 26 maggio 2020, inizialmente come intercettazione telefonica, si è conclusa nel mese di maggio 2024, sotto il controllo dei Governi Draghi e Meloni che si sono succeduti dalla data della prima autorizzazione. Con riferimento a tale operazione, l'utilizzo del captatore informatico *Graphite* risulta essere stato autorizzato in data 5 settembre 2024 dall'Autorità delegata, Sottosegretario Alfredo Mantovano. In entrambi i casi, risulta peraltro rispettata la procedura delineata dall'articolo 4 del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, che prevede l'autorizzazione del Procuratore generale presso la Corte di appello di Roma per lo svolgimento dell'attività di intercettazione.

In tale seconda operazione risulta essere stato altresì sottoposto ad attenzione da parte degli organismi Giuseppe Caccia.

Con riferimento alle posizioni di Luca Casarini e Giuseppe Caccia, secondo quanto riferito nelle audizioni svolte, oltre al rispetto della citata normativa in materia di intercettazioni preventive e di garanzie funzionali, è stato altresì evidenziato il rispetto anche dei termini contrattuali sopra richiamati in quanto tali soggetti sono stati sottoposti ad attività intercettiva non in qualità di attivisti per i diritti umani, ma in riferimento alle loro attività potenzialmente relative all'immigrazione irregolare.

Con riferimento, invece, alla posizione del giornalista Francesco Cancellato, sulla base degli elementi acquisiti e dalle verifiche svolte dal Comitato risulta che questi non sia stato sottoposto ad alcun tipo di attenzione da parte dei servizi di informazione per la sicurezza italiani attraverso l'utilizzo dello *spyware* prodotto dalla società *Paragon*. Il Comitato ha avuto peraltro modo di verificare direttamente, nel corso dei sopralluoghi svolti presso AISI e AISE e presso la Procura generale presso la Corte di appello di Roma, la mancata sottoposizione del giornalista Cancellato ad attività intercettiva da parte dei servizi di informazione per la sicurezza.

In particolare, nel corso dei sopralluoghi effettuati presso le due Agenzie, i componenti del Comitato, come segnalato sopra, hanno potuto interrogare direttamente il *database* e il registro di *audit* del sistema *Paragon*, inserendo il numero dell'utenza del giornalista oggetto dell'*alert* di *WhatsApp* acquisito autonomamente dal Comitato stesso, constatando l'assenza di qualunque attività intercettiva attraverso l'utilizzo dello *spyware Graphite* relativamente a tale utenza.

I componenti del Comitato hanno avuto altresì la possibilità di verificare, nel corso dei sopralluoghi presso il DIS e presso la Procura generale presso la Corte d'appello di Roma, l'assenza di richieste di autorizzazione, ovvero di decreti di autorizzazione relativi alla sottoposizione del giornalista a qualsivoglia attività intercettiva da parte dei servizi italiani, sia attraverso lo strumento delle intercettazioni telefoniche che attraverso quello delle garanzie funzionali, anche a prescindere dall'utilizzo dello *spyware Graphite*.

Inoltre, anche nel rapporto di *The CitizenLab*, pubblicato il 19 marzo 2025, non vi è conferma diretta di infezione del dispositivo mobile del giornalista, mentre viene riportata conferma espressa dell'infezione, sulla base di analisi forensi già conclusesi, limitatamente ai dispositivi di Casarini e Caccia. Nel corso delle audizioni svoltesi, è peraltro emerso che tale indagine forense con riferimento al dispositivo del giornalista Cancellato sarebbe ancora in corso, senza che al momento sia stato possibile rilevare tracce dell'indicatore informatico (*BIGPRETZEL*) utilizzato dal laboratorio canadese per dimostrare infezioni riconducibili allo *spyware* prodotto da *Paragon*. Sulla base delle informazioni emerse nel corso delle audizioni, l'unico elemento che, allo stato, confermerebbe un'eventuale intrusione nel dispositivo di Cancellato, peraltro non espressamente attribuita al *software Graphite*, sarebbe rappresentato dalla notifica ricevuta sul dispositivo del giornalista. Sulla questione il laboratorio *The CitizenLab* si è comunque riservato di pubblicare, non appena saranno disponibili, gli esiti dell'indagine forense, che saranno eventualmente oggetto di approfondimento da parte del Comitato.

I rappresentanti del laboratorio, nel corso di un'audizione svoltasi presso la Commissione libertà civili, giustizia e affari interni del Parlamento europeo il 13 maggio 2025 e poi anche in una nota trasmessa al Comitato in data 16 maggio 2025, hanno indicato il giornalista Cancellato come un *target Paragon* confermato, senza tuttavia precisare se tali affermazioni siano suffragate dalla effettiva conclusione della richiamata analisi forense, ma richiamando, in risposta ad una domanda posta nel corso della citata audizione, solo la notifica effettuata da Meta. Tuttavia, sulla base degli elementi emersi nelle audizioni svolte e della documentazione acquisita dal Comitato, risulta che la società Meta non possa determinare chi sospetta sia stato coinvolto dallo *spyware Graphite* con assoluta sicurezza.

In proposito, fermo restando che, sulla base delle verifiche sopra descritte, il giornalista Cancellato non risulta essere stato oggetto di attenzione da parte dei servizi italiani, si ricorda che, come evidenziato sopra, le utenze con prefisso italiano non rientrano tra quelle per le quali è esclusa contrattualmente la sottoposizione a captazione attraverso lo *spyware Graphite*.

In proposito, nel corso delle audizioni è emerso come il laboratorio canadese abbia potuto divulgare l'esito degli accertamenti effettuati con esclusivo riferimento ai soggetti che avevano espressamente prestato consenso alla diffusione della propria identità.

Non risultano sottoposti ad attività intercettiva da parte dei servizi di informazione per la sicurezza apparati in uso a don Mattia Ferrari. Risulterebbe, invece, essere stata oggetto di attenzione da parte dei servizi un'utenza nella disponibilità di David Yambio, tuttavia intestata a don Mattia Ferrari. Tale operazione è stata comunque effettuata senza ricorrere all'utilizzo dello *spyware Graphite*. In particolare, il citato cittadino sudanese è stato sottoposto ad attività intercettiva da parte degli organismi di informazione dal 24 luglio 2023 all'8 aprile 2024, nell'ambito di un'operazione autorizzata con una delega del 26 maggio 2020. Come riportato dai *media* e confermato nell'ambito dell'attività istruttoria svolta dal Comitato, il cittadino sudanese risulta peraltro oggetto di attività intercettiva disposta dall'autorità giudiziaria nell'ambito di un procedimento penale. Tale ultima questione evidentemente esula dalle competenze del Comitato e non può quindi formare oggetto della presente relazione.

4. Approfondimento della disciplina delle intercettazioni preventive dei servizi.

La vicenda oggetto della presente relazione ha consentito al Comitato di svolgere un approfondimento anche di carattere generale sulla disciplina delle intercettazioni preventive svolte dai servizi di informazione per la sicurezza.

Com'è noto la materia è disciplinata dall'articolo 4 del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, che, in particolare al comma 1, prevede la facoltà per il Presidente del Consiglio di delegare i direttori dei servizi a richiedere l'autorizzazione all'intercettazione di comunicazioni o conversazioni, anche per via telematica, nonché all'intercettazione di comunicazioni o conversazioni tra presenti, anche se queste avvengono in un domicilio privato, quando siano ritenute indispensabili per l'espletamento delle attività affidate alle Agenzie dagli articoli 6 e 7 della legge 3 agosto 2007, n. 124. Il successivo comma 2 stabilisce che la richiesta di autorizzazione è rivolta al Procuratore generale presso la Corte di appello di Roma.

Sul punto, si ricorda che la Procura generale di Roma, il 28 maggio 2024, ha adottato apposite linee guida in materia di intercettazioni preventive svolte dai servizi, precisando, tra l'altro, i requisiti necessari per la concessione dell'autorizzazione al fine di bilanciare i diversi diritti costituzionalmente garantiti che risultano incisi da tale attività.

Tale sistema riguarda, come è noto, le intercettazioni relative alle conversazioni in corso.

La lettera della richiamata disposizione di cui all'articolo 4, comma 1, del citato decreto-legge n. 144 del 2005, convertito, con modificazioni, dalla legge n. 155 del 2005, prevede infatti la sottoposizione all'autorizzazione del Procuratore generale presso la Corte di appello di Roma per le sole intercettazioni di conversazioni o comunicazioni, effettuate anche in via telematica, oltre alle intercettazioni ambientali.

L'utilizzo di captatori informatici, che hanno un'efficacia ben più invasiva delle tradizionali intercettazioni telefoniche, consente tuttavia di acquisire non solo i contenuti di conversazioni telefoniche anche effettuate attraverso strumenti con tecnologia *VoIP*, ma anche i messaggi scambiati con le diverse applicazioni a disposizione ovvero ogni altro contenuto che sia presente sul dispositivo mobile infettato dal cosiddetto *spyware*.

La giurisprudenza relativa all'attività di captazione, a prescindere dalla particolare fattispecie delle intercettazioni preventive dei servizi, aveva distinto tra comunicazioni captate nell'ambito di un flusso dinamico, che rientrano certamente nella nozione di comunicazioni ai fini del rispetto dell'articolo 15, secondo comma, della Costituzione, che prescrive il vaglio dell'autorità giudiziaria per limitare la segretezza delle comunicazioni stesse, e messaggi archiviati sul dispositivo mobile, che rientrerebbero viceversa nella categoria della documentazione, priva quindi della garanzia di cui al richiamato articolo 15 della Costituzione.

Per l'esfiltrazione di messaggi, ovvero di dati informatici comunque presenti sui dispositivi mobili, come peraltro confermato nell'ambito delle audizioni, risulta, allo stato, prevista la sola autorizzazione del Presidente del Consiglio dei ministri, ovvero dell'Autorità delegata, rilasciata ai sensi dell'articolo 18, comma 2, della legge n. 124 del 2007, senza alcun vaglio da parte dell'autorità giudiziaria, sia pure nella particolare accezione delineata dal decreto-legge n. 144 del 2005, convertito, con modificazioni, dalla legge n. 155 del 2005, ossia di autorità terza e indipendente.

Tale impostazione appare meritevole di un approfondimento alla luce della recente sentenza della Corte costituzionale 7 giugno 2023, n. 170, che ha stabilito come i messaggi archiviati sul dispositivo mobile che rivestano un interesse attuale per il proprietario siano da considerarsi come corrispondenza e come tali ricadenti nella disciplina dell'articolo 15 della Costituzione, che ne tutela la segretezza, salvo provvedimento motivato dell'autorità giudiziaria.

5. Conclusioni

Come già ricordato nella presente relazione, l'oggetto del controllo esercitato dal Comitato è, ai sensi dell'articolo 30, comma 2, della legge n. 124 del 2007, quello di « verificare, in modo sistematico e continuativo, che l'attività del Sistema di informazione per la sicurezza si svolga nel rispetto della Costituzione, delle leggi, nell'esclusivo interesse e per la difesa della Repubblica e delle sue istituzioni ».

Sotto tale profilo, l'ampia e approfondita analisi svolta consente di affermare, sulla base di quanto risulta agli atti del Comitato e dall'attività istruttoria effettuata, che l'attività dei servizi di informazione si è svolta secondo i parametri indicati dalla citata disposizione.

È opportuno sottolineare come il Comitato abbia dispiegato la propria attività istruttoria in maniera analitica e scrupolosa attraverso le audizioni dei soggetti istituzionali e privati interessati dalla vicenda, l'analisi puntuale di documenti presenti negli archivi del DIS e della Procura generale della Repubblica presso la Corte d'appello di Roma, nonché attraverso la consultazione diretta del *database* e del registro di

audit dello *spyware Graphite* presso le sedi di AISE e AISI, attivando la procedura di cui all'articolo 31, comma 14, della legge n. 124 del 2007, che consente al Comitato, previa comunicazione al Presidente del Consiglio, di effettuare « accessi e sopralluoghi negli uffici di pertinenza del Sistema di informazione per la sicurezza ».

In particolare, sulla base di tale istruttoria, risulta al Comitato che l'attività informativa posta in essere dai servizi di informazione per la sicurezza nei confronti di Luca Casarini, Giuseppe Caccia e David Yambio è stata autorizzata nelle forme e nei limiti previsti, con riferimento all'utilizzo delle garanzie funzionali, dagli articoli 17 e 18 della legge n. 124 del 2007, ovvero con decreto dell'Autorità delegata, e, con riferimento alle intercettazioni, dall'articolo 4, commi 1 e 2, del decreto-legge n. 144 del 2005, convertito, con modificazioni, dalla legge n. 155 del 2005, ovvero su autorizzazione del Procuratore generale presso la Corte d'appello di Roma.

Come specificato nella sezione 3.1 del terzo capitolo della presente relazione, in particolare, sulla base dell'istruttoria svolta risulta che tali attività si siano dispiegate nell'ambito di due distinte operazioni. La prima, la cui delega è stata rilasciata il 23 dicembre 2019 dal Presidente del Consiglio dei ministri *pro tempore*, per essere successivamente autorizzata dal Procuratore generale della Repubblica presso la Corte di appello di Roma, si è conclusa nel mese di marzo 2020, coinvolgendo Luca Casarini e Giuseppe Caccia. La seconda, di natura più ampia, la cui delega è stata rilasciata dal Presidente del Consiglio dei ministri *pro tempore* il 26 maggio 2020, si è conclusa nel mese di maggio 2024, previe autorizzazioni del Procuratore generale presso la Corte d'appello di Roma per le parti di competenza e sulle successive proroghe. Nell'ambito di tale operazione risulta attenzionato, oltre ai suddetti Casarini e Caccia, anche il cittadino sudanese David Yambio.

Con specifico riferimento al caso del giornalista Francesco Cancellato, si ricordano in premessa i seguenti elementi acquisiti dal Comitato nel corso dell'attività istruttoria condotta e riportati nel testo della presente relazione. In primo luogo, il laboratorio canadese *The CitizenLab*, nel corso dell'audizione del 16 aprile 2025 ha affermato come, mentre l'infezione ad opera dello *spyware Graphite* poteva essere confermata con riferimento ai dispositivi mobili di Luca Casarini e Giuseppe Caccia, sulla base di specifiche analisi forensi condotte sui rispettivi dispositivi mobili, analoga conferma non poteva essere data con riferimento al dispositivo di Francesco Cancellato, pure aggiungendo che non era conclusa la relativa analisi forense. Successivamente, gli stessi rappresentanti del laboratorio canadese, nel corso della richiamata audizione svoltasi presso la Commissione libertà civili, giustizia e affari interni del Parlamento europeo il 13 maggio 2025, oltre a opinioni che travalicano i profili tecnici, hanno indicato il giornalista Cancellato come un *target Paragon* confermato, senza tuttavia precisare se tale affermazione fosse suffragata dalla effettiva conclusione della richiamata analisi forense, ma richiamando, in risposta ad una domanda posta nel corso della citata audizione, solo la notifica effettuata da Meta. Sul punto, si ricorda che la società Meta ha chiarito al Comitato che non può determinare con assoluta sicurezza chi sospetta sia stato coinvolto dallo *spyware* prodotto da *Paragon Solutions*. Lo stesso laboratorio, in una nota trasmessa al Comitato il

16 maggio 2025, qualifica nuovamente Francesco Cancellato come un *target Paragon* confermato senza alcuna specificazione al riguardo.

Ciò premesso, sulla base dell'ampia attività conoscitiva svolta nel corso delle audizioni, della documentazione acquisita e delle verifiche effettuate presso le sedi di DIS, AISE e AISI, nonché presso gli uffici della Procura generale presso la Corte di appello di Roma, che hanno consentito ai componenti del Comitato di esaminare direttamente la documentazione relativa alle autorizzazioni allo svolgimento di intercettazioni o di condotte previste dalla legge come reato, il Comitato ha accertato che il giornalista Francesco Cancellato non è stato sottoposto ad attività intercettiva da parte dei servizi di informazione per la sicurezza italiani mediante l'utilizzo dello *spyware Graphite*, né risulta nei suoi confronti autorizzata nessuna altra forma di attività informativa da parte degli stessi organismi.

Parimenti, sulla base dell'istruttoria effettuata, non risulta al Comitato alcuna attività informativa da parte dei servizi di informazione per la sicurezza italiani in relazione ad utenze in uso al sacerdote don Mattia Ferrari.

Si segnala, come peraltro riportato nel secondo capitolo della presente relazione, che, sulla base di quanto emerso nel corso dell'attività istruttoria, la società *Paragon Solutions* ha dichiarato di fornire i propri servizi ad operatori governativi presenti in numerosi Stati e che non risultano esservi restrizioni tecniche o contrattuali sulla possibilità di utilizzare il citato *spyware* con riferimento ad utenze aventi prefisso italiano.

Come chiarito anche sopra, non possono formare oggetto della presente relazione le attività di indagine in corso presso alcune Procure della Repubblica, i cui esiti il Comitato si riserva comunque di valutare qualora emergessero profili di competenza.

Non risulta inoltre al Comitato che ricorra una fattispecie di violazione dell'articolo 8, comma 1, della legge n. 124 del 2007 – che prevede l'esclusività delle funzioni degli organismi, di cui il Comitato, ai sensi dell'articolo 30, comma 2-*bis*, della medesima legge è chiamato ad accertare il rispetto – in quanto non è emerso, allo stato, che soggetti privati abbiano esercitato abusivamente le funzioni attribuite dalla legge al Comparto.

L'ampio spettro dell'indagine svolta dal Comitato ha consentito, inoltre, di valutare alcuni profili di carattere giuridico relativi all'esecuzione di operazioni di captazione informatica preventiva.

In primo luogo, come emerso dalla stessa vicenda oggetto dell'indagine, le società di messaggistica, nel comprensibile, condivisibile e doveroso obiettivo di salvaguardare prioritariamente la riservatezza dei propri utenti, possono tuttavia trovarsi a disvelare, come in alcuni dei casi trattati nella presente relazione, operazioni degli apparati di *intelligence*, legittimamente autorizzate, nel rispetto della Costituzione e delle leggi italiane ovvero, in astratto, anche indagini della magistratura parimenti legittime, con potenziale pregiudizio per le operazioni stesse o per le indagini.

La questione è particolarmente delicata e risiede *in re ipsa* nella differenza tra le classiche intercettazioni telefoniche, che presuppongono una collaborazione con il gestore telefonico nelle forme previste dalla legge, e l'inoculazione di *spyware* o *trojan* che hanno come

obiettivo quello di utilizzare il dispositivo mobile dell'utente *target* come captatore di conversazioni o messaggistica archiviate anche su piattaforme diverse e quindi gestite da operatori diversi, che spesso, come chiarito nel corso delle audizioni, nemmeno dispongono dei dati relativi all'identità degli utenti stessi.

Come evidenziato nel corso delle audizioni, le società che offrono servizi di messaggistica istantanea e comunicazioni *VoIP*, come peraltro anche i fornitori dei principali sistemi operativi per dispositivi mobili – operatori globali presenti in contesti nazionali molto diversi, compresi Paesi che non hanno stringenti regolazioni sulla riservatezza, al contrario dell'Unione europea – oltre al rispetto delle leggi vigenti, si vincolano anche al rispetto di *policy* aziendali sulla base delle quali si riservano o meno di corrispondere ad eventuali richieste delle pubbliche autorità. Tali limitazioni, se possono essere considerate un presidio di tutela della libertà degli utenti in regimi autoritari, non possono tradursi in condotte potenzialmente idonee ad incidere sulla sicurezza nazionale in contesti, come quello italiano ed europeo, in cui le autorità sono chiamate ad esercitare i pubblici poteri nello scrupoloso rispetto della Costituzione e dei limiti imposti dallo Stato di diritto.

Il Comitato invita quindi le Camere e il Governo ad approfondire tale questione anche al fine di adottare le opportune iniziative di carattere normativo volte ad impedire il disvelamento di operazioni e indagini pienamente legittime, anche individuando soggetti istituzionali che possano verificare, prima della comunicazione agli utenti, la legittimità di eventuali manovre intercettive. In considerazione della natura globale degli operatori interessati, l'introduzione di regole di questo genere dovrebbe avvenire promuovendo anche una uniforme regolamentazione in sede europea e internazionale.

Il secondo aspetto su cui il Comitato invita il Parlamento e il Governo ad adottare opportune iniziative *de iure condendo* è relativo agli effetti della citata sentenza della Corte costituzionale 7 giugno 2023, n. 170, che, come riportato *supra*, ha stabilito che le conversazioni archiviate sui dispositivi mobili siano da qualificarsi come corrispondenza e come tali ricadenti nell'ambito di applicazione dell'articolo 15 della Costituzione.

In particolare, la richiamata sentenza della Corte costituzionale impone una riflessione sull'opportunità, come peraltro emerso nel corso dell'interlocuzione con la Procura generale presso la Corte di appello di Roma, di una revisione normativa volta a prevedere l'estensione della necessità di autorizzazione del Procuratore generale presso la Corte di appello di Roma, prevista ai sensi dell'articolo 4, comma 2, del decreto-legge n. 144 del 2005, convertito, con modificazioni, dalla legge n. 155 del 2005, anche all'acquisizione di messaggi o altri dati informatici già presenti sugli apparati oggetto dell'attività informativa, ancorché non rientranti nella nozione di comunicazioni in senso stretto, essendo fuori da un flusso dinamico di scambio.

Altra questione di carattere giuridico legata all'utilizzo delle moderne tecnologie di captazione, che, come emerso dalle audizioni, comportano il salvataggio di dati su *database* non cancellabili da parte dei soggetti pubblici utilizzatori, se non con il concorso del fornitore del servizio, riguarda la necessità di individuare modalità per garantire il rispetto delle disposizioni di cui all'articolo 4-*bis*, commi 3 e 4, del

decreto-legge n. 155 del 2005, convertito, con modificazioni, dalla legge n. 144 del 2005, che prevedono la distruzione di tutto il materiale acquisito nel corso delle operazioni di intercettazione con la sola eccezione dei decreti di autorizzazione emanati dal Procuratore generale presso la Corte di appello di Roma.

Anche con riferimento a tale questione, il Comitato invita le Camere ad avviare una riflessione sull'opportunità di adottare iniziative normative volte a garantire l'effettiva distruzione dei contenuti intercettati attraverso l'utilizzo delle più sofisticate tecnologie di captazione.

L'attività di approfondimento condotta dal Comitato ha consentito, infine, di effettuare, a quasi venti anni dalla data di entrata in vigore della legge n. 124 del 2007, una riflessione sui poteri di controllo attribuiti al Comitato. Su quest'ultimo aspetto il Comitato invita le Camere ad una riflessione sull'opportunità di adottare alcune integrazioni puntuali alla richiamata legge n. 124 del 2007 con riferimento al controllo parlamentare sugli organismi di informazione per la sicurezza. In proposito, potrebbero essere ulteriormente rafforzati alcuni obblighi informativi preventivi, nonché il livello di dettaglio degli elementi messi a disposizione del Comitato dopo la conclusione di operazioni coperte da garanzie funzionali ovvero di operazioni di intercettazioni autorizzate dal Procuratore generale presso la Corte d'appello di Roma.

190340146570