# DECISIONI

## DECISIONE (UE) 2022/480 DEL PARLAMENTO EUROPEO

**del 10 marzo 2022**

**sulla costituzione, le attribuzioni, la composizione numerica e la durata del mandato della commissione d'inchiesta incaricata di esaminare l'uso di Pegasus e di spyware di sorveglianza equivalenti, nonché sulla definizione dell'oggetto dell'inchiesta**

IL PARLAMENTO EUROPEO,

— vista la richiesta presentata da 290 deputati di istituire una commissione d'inchiesta incaricata di esaminare ed indagare le denunce di infrazione o di cattiva amministrazione nell'applicazione del diritto dell'Unione per quanto riguarda l'uso di Pegasus e di spyware di sorveglianza equivalenti installati su dispositivi mobili sfruttando le vulnerabilità informatiche («spyware di sorveglianza equivalenti»),

— vista la proposta della Conferenza dei presidenti,

— visto l'articolo 226 del trattato sul funzionamento dell'Unione europea (TFUE),

— vista la decisione 95/167/CE, Euratom, CECA del Parlamento europeo, del Consiglio e della Commissione, del 19 aprile 1995, relativa alle modalità per l'esercizio del diritto d'inchiesta del Parlamento europeo ([1]),

— visto l'impegno dell'Unione europea a favore dei valori e dei principi di libertà, democrazia e rispetto dei diritti umani e delle libertà fondamentali e dello Stato di diritto, come indicato nel preambolo del trattato sull'Unione europea (TUE), in particolare agli articoli 2, 6 e 21,

— visto l'articolo 4, paragrafo 2, TUE, che ribadisce la competenza esclusiva degli Stati membri per il mantenimento dell'ordine pubblico e la tutela della sicurezza nazionale,

— visti gli articoli 16 e 223 TFUE,

— vista la Carta dei diritti fondamentali dell'Unione europea («Carta»), in particolare gli articoli 7, 8, 11, 21 e 47 — che riconoscono i diritti, le libertà e i principi specifici in essa sanciti quali il rispetto della vita privata e familiare e la protezione dei dati di carattere personale, la libertà di espressione e di informazione, il diritto alla non discriminazione, nonché il diritto a un ricorso effettivo e a un giudice imparziale —, i quali si applicano pienamente agli Stati membri nell'attuazione del diritto dell'Unione, e visto il suo articolo 52, paragrafo 1, che consente talune limitazioni all'esercizio dei diritti e delle libertà fondamentali,

— vista la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) ([2]),

— visto il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) ([3]),

— vista la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio ([4]),

([1]) GU L 113 del 19.5.1995, pag. 1.
([2]) GU L 201 del 31.7.2002, pag. 37.
([3]) GU L 119 del 4.5.2016, pag. 1.
([4]) GU L 119 del 4.5.2016, pag. 89.

— vista la decisione (PESC) 2019/797 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri ([5]), quale modificata dalla decisione (PESC) 2021/796 del Consiglio del 17 maggio 2021 ([6]),

— visto il regolamento (UE) 2021/821 del Parlamento europeo e del Consiglio, del 20 maggio 2021, che istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso ([7]),

— visto l'atto relativo all'elezione dei membri del Parlamento europeo a suffragio universale diretto ([8]),

— visti la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, in particolare gli articoli 8, 9, 13 e 17, e i relativi protocolli,

— visti i principi guida delle Nazioni Unite su imprese e diritti umani ([9]),

— viste la sua risoluzione del 12 marzo 2014 sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sui diritti fondamentali dei cittadini dell'UE, e sulla cooperazione transatlantica nel campo della giustizia e degli affari interni ([10]), e le sue raccomandazioni riguardanti il rafforzamento della sicurezza informatica nelle istituzioni, organi e agenzie dell'UE,

— visto l'articolo 208 del proprio regolamento,

A. considerando che da recenti rivelazioni risulta che diversi paesi, tra cui degli Stati membri, hanno utilizzato lo spyware di sorveglianza Pegasus contro giornalisti, politici, funzionari delle autorità di contrasto, diplomatici, avvocati, imprenditori, attori della società civile e altri attori, e che tali pratiche sono estremamente allarmanti e sembrano confermare i pericoli dell'uso improprio della tecnologia di sorveglianza per minare i diritti umani e la democrazia;

1. decide di costituire una commissione d'inchiesta incaricata di esaminare le denunce di infrazione o di cattiva amministrazione nell'applicazione del diritto dell'Unione, fatte salve le prerogative delle giurisdizioni nazionali o dell'Unione;

2. decide che la commissione d'inchiesta sarà incaricata di:

— indagare sulla portata dei presunti casi di infrazione o cattiva amministrazione nell'attuazione del diritto dell'Unione derivanti dall'uso di Pegasus e di spyware di sorveglianza equivalenti, raccogliere informazioni sulla misura in cui Stati membri, comprese, ma non solo, l'Ungheria e la Polonia, o paesi terzi usano una sorveglianza intrusiva con modalità che violano i diritti e le libertà sanciti dalla Carta, nonché valutare il livello di rischio che ciò comporta per i valori sanciti dall'articolo 2 TUE, come la democrazia, lo Stato di diritto e il rispetto dei diritti umani;

— per l'esercizio delle sue funzioni, raccogliere e analizzare informazioni per accertare:

— l'uso e il funzionamento di Pegasus e di spyware di sorveglianza equivalenti e il loro presunto impatto negativo sui diritti fondamentali sanciti dalla Carta, nell'attuazione da parte degli Stati membri del diritto dell'Unione;

— il quadro giuridico esistente in cui gli Stati membri hanno acquisito e utilizzato Pegasus e spyware di sorveglianza equivalenti;

— se le autorità degli Stati membri hanno utilizzato Pegasus e spyware di sorveglianza equivalenti per scopi politici, economici o altri scopi ingiustificati per spiare giornalisti, politici, funzionari delle forze di contrasto, diplomatici, avvocati, imprenditori, attori della società civile o altri attori, in violazione del diritto dell'Unione e dei valori sanciti dall'articolo 2 TUE o dei diritti sanciti dalla Carta;

([5]) GU L 129 I del 17.5.2019, pag. 13.
([6]) GU L 174 I del 18.5.2021, pag. 1.
([7]) GU L 206 dell'11.6.2021, pag. 1.
([8]) GU L 278 dell'8.10.1976, pag. 5.
([9]) https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
([10]) GU C 378 del 9.11.2017, pag. 104.

— se l'utilizzo, in violazione del diritto dell'Unione, di Pegasus e di spyware di sorveglianza equivalenti abbia avuto un impatto negativo sui processi democratici negli Stati membri per quanto riguarda le elezioni a livello locale, nazionale ed europeo;

— i presunti casi di infrazione della direttiva 2002/58/CE o di cattiva amministrazione da parte di Stati membri derivanti dall'uso di Pegasus e di spyware di sorveglianza equivalenti, in particolare per quanto riguarda il principio di riservatezza delle comunicazioni e il divieto di ascoltare, intercettare, memorizzare o altri tipi di intercettazione o sorveglianza delle comunicazioni e dei relativi dati sul traffico delle persone;

— se l'uso di Pegasus e di spyware di sorveglianza equivalenti da parte degli Stati membri abbia costituito, comportato o rivelato violazioni della direttiva (UE) 2016/680 e del regolamento (UE) 2016/679;

— se la Commissione disponeva di prove dell'uso di Pegasus e di spyware di sorveglianza equivalenti contro persone;

— se gli Stati membri abbiano assicurato salvaguardie istituzionali e giuridiche sufficienti per evitare l'uso illegale di spyware e se le persone che sospettano che i loro diritti siano stati violati dall'uso di spyware abbiano accesso a mezzi di ricorso efficaci;

— la presunta inazione degli Stati membri rispetto al coinvolgimento di entità dell'UE nello sviluppo, nella diffusione o nel finanziamento di Pegasus e di spyware di sorveglianza equivalenti, compresa la catena di approvvigionamento in termini di tecnologia e il suo sfruttamento, nella misura in cui ciò è in violazione del diritto dell'Unione, compreso il regolamento (UE) 2021/821, e anche quando software di sorveglianza commercializzati per un certo scopo (ad esempio la lotta contro il terrorismo) sono utilizzati in un altro contesto;

— il ruolo del governo di Israele e di altri paesi terzi nel fornire agli Stati membri Pegasus e spyware di sorveglianza equivalenti;

— se l'uso di Pegasus o spyware di sorveglianza equivalenti da parte delle autorità degli Stati membri abbia comportato il trasferimento di dati personali verso paesi terzi, in particolare, ma non solo, al gruppo NSO e a governi di paesi terzi;

— se l'uso di Pegasus o spyware di sorveglianza equivalenti, che coinvolge direttamente o indirettamente entità collegate all'UE, abbia contribuito a spiare illegalmente giornalisti, politici, funzionari delle autorità di contrasto, diplomatici, avvocati, imprenditori, attori della società civile o altri attori in paesi terzi e abbia portato a violazioni o abusi dei diritti umani che destano grave preoccupazione per quanto riguarda gli obiettivi della politica estera e di sicurezza comune dell'UE, e se tale uso sia stato in violazione dei valori sanciti dall'articolo 21 TUE e dalla Carta, anche tenendo debitamente conto dei principi guida delle Nazioni Unite su imprese e diritti umani e di altri diritti sanciti dal diritto internazionale in materia di diritti umani;

— se vi erano motivi sufficienti per giustificare l'adozione da parte del Consiglio di misure restrittive o sanzioni nel quadro della politica estera e di sicurezza comune dell'UE nei confronti di uno o più paesi terzi qualora una decisione, adottata conformemente al titolo V, capo 2, TUE, preveda l'interruzione o la riduzione delle relazioni economiche o finanziarie, a norma dell'articolo 215, paragrafo 1, TFUE;

— se l'uso di Pegasus o spyware di sorveglianza equivalenti da parte di paesi terzi abbia avuto un impatto sui diritti fondamentali garantiti dal diritto dell'Unione e se vi fossero motivi sufficienti perché il Consiglio riesaminasse eventuali accordi di cooperazione internazionale nello spazio di libertà, sicurezza e giustizia conclusi con paesi terzi a norma dell'articolo 218 TFUE;

— presentare le eventuali raccomandazioni che riterrà opportune al riguardo;

— formulare raccomandazioni per proteggere le istituzioni dell'UE, i suoi membri e il personale da tali spyware di sorveglianza;

3. decide che la commissione d'inchiesta presenterà la sua relazione entro un termine di 12 mesi dall'approvazione della presente decisione;
4. decide che la commissione d'inchiesta dovrà tener conto nel proprio lavoro degli eventuali sviluppi pertinenti di sua competenza che dovessero intervenire durante il suo mandato;
5. sottolinea che, al fine di garantire una buona cooperazione e un buon flusso di informazioni tra la commissione d'inchiesta e le commissioni e sottocommissioni permanenti competenti, il presidente e il relatore della commissione d'inchiesta potrebbero essere coinvolti nelle pertinenti discussioni delle commissioni e sottocommissioni permanenti e viceversa, in particolare per le audizioni della commissione d'inchiesta;
6. decide che eventuali raccomandazioni elaborate dalla commissione d'inchiesta vengano deferite alle pertinenti commissioni e sottocommissioni permanenti nei rispettivi settori di competenza, quali definiti all'allegato VI del regolamento;
7. decide che la commissione d'inchiesta sarà composta di 38 membri;
8. incarica la sua presidente di provvedere alla pubblicazione della presente decisione nella *Gazzetta ufficiale dell'Unione europea*.