DECISIONI

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

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato dell'Unione europea, in particolare l'articolo 29,

vista la proposta dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza,

considerando quanto segue:

(1) Il 19 giugno 2017 il Consiglio ha adottato le conclusioni su un quadro relativo a una risposta diplomatica comune alle attività informatiche dolose («pacchetto di strumenti della diplomazia informatica»), nelle quali il Consiglio ha espresso preoccupazione per le crescenti capacità e volontà degli attori statali e non statali di perseguire i propri obiettivi intraprendendo attività informatiche dolose e ha affermato la crescente necessità di proteggere l'integrità e la sicurezza dell'Unione, dei suoi Stati membri e dei loro cittadini dalle minacce informatiche e dalle attività informatiche dolose.

(2) Il Consiglio ha sottolineato che segnalare in modo chiaro le probabili conseguenze di una risposta diplomatica comune dell'Unione a tali attività informatiche dolose influenza il comportamento dei potenziali aggressori nel ciberspazio, rafforzando così la sicurezza dell'Unione e dei suoi Stati membri. Ha inoltre affermato che le misure nell'ambito della politica estera e di sicurezza comune (PESC), comprese ove necessario le misure restrittive adottate ai sensi delle pertinenti disposizioni dei trattati, sono adeguate per un quadro relativo a una risposta diplomatica comune alle attività informatiche dolose, al fine di incoraggiare la cooperazione, facilitare la riduzione delle minacce immediate e a lungo termine, e influenzare il comportamento dei potenziali aggressori sul lungo periodo.

(3) L'11 ottobre 2017 il comitato politico e di sicurezza ha approvato le linee guida di attuazione del pacchetto di strumenti della diplomazia informatica. Le linee guida di attuazione fanno riferimento a cinque categorie di misure, incluse le misure restrittive, nell'ambito del pacchetto di strumenti della diplomazia informatica, e alla procedura per invocare dette misure.

(4) Nelle conclusioni del 16 aprile 2018 sulle attività informatiche dolose il Consiglio ha condannato fermamente l'uso illecito di tecnologie dell'informazione e della comunicazione (TIC) e ha sottolineato che l'uso delle TIC a fini dolosi è inaccettabile dal momento che compromette la stabilità, sicurezza e i vantaggi offerti da Internet e dall'uso delle TIC. Il Consiglio ha ricordato che il pacchetto di strumenti della diplomazia informatica contribuisce alla prevenzione dei conflitti, alla cooperazione e alla stabilità nel ciberspazio delineando le misure nell'ambito della PESC, incluse le misure restrittive, che possono essere usate per prevenire e rispondere a tali attività. Ha dichiarato che l'Unione continuerà con decisione a difendere l'applicabilità del diritto internazionale esistente al ciberspazio e ha sottolineato che il rispetto del diritto internazionale, in particolare della Carta delle Nazioni Unite, è fondamentale per mantenere la pace e la stabilità. Il Consiglio ha inoltre sottolineato che gli Stati non devono servirsi di proxy per commettere atti illeciti a livello internazionale mediante l'uso delle TIC e dovrebbero cercare di assicurare che il loro territorio non sia utilizzato da attori non statali per commettere tali atti, come indicato nella relazione del 2015 del gruppo di esperti governativi delle Nazioni Unite sugli sviluppi nel settore dell'informazione e delle telecomunicazioni nel contesto della sicurezza internazionale.

(5) Il 28 giugno 2018 il Consiglio europeo ha adottato conclusioni in cui sottolinea la necessità di rafforzare le capacità di combattere le minacce alla cibersicurezza provenienti dall'esterno dell'Unione. Il Consiglio europeo ha chiesto alle istituzioni e agli Stati membri di attuare le misure indicate nella comunicazione congiunta della Commissione e dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza del 13 giugno 2018 dal titolo «Rafforzamento della resilienza e potenziamento delle capacità di affrontare minacce ibride», compreso l'uso pratico del pacchetto di strumenti della diplomazia informatica.

(6) Il 18 ottobre 2018 il Consiglio europeo, facendo seguito alle conclusioni del Consiglio del 19 giugno 2017, ha adottato conclusioni in cui si chiedeva di portare avanti i lavori sulla capacità di scoraggiare gli attacchi informatici e di rispondervi attraverso misure restrittive dell'Unione.

(7) In tale contesto, la presente decisione istituisce un quadro per misure restrittive mirate volte a scoraggiare e contrastare gli attacchi informatici con effetti significativi, che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri. Ove ritenuto necessario ai fini del conseguimento degli obiettivi della PESC enunciati nelle pertinenti disposizioni dell'articolo 21 del trattato sull'Unione europea, la presente decisione consente altresì misure restrittive che devono essere applicate in risposta ad attacchi informatici con effetti significativi nei confronti di Stati terzi o organizzazioni internazionali.

(8) Affinché abbiano un effetto deterrente e dissuasivo, le misure restrittive mirate dovrebbero incentrarsi sugli attacchi informatici rientranti nell'ambito di applicazione della presente decisione che sono sferrati in modo deliberato.

(9) È opportuno distinguere le misure restrittive mirate dall'attribuzione a uno Stato terzo della responsabilità per gli attacchi informatici. L'applicazione di misure restrittive mirate non equivale a tale attribuzione, che è una decisione politica sovrana adottata caso per caso. Ciascuno Stato membro può decidere liberamente in merito all'attribuzione degli attacchi informatici a uno Stato terzo.

(10) È necessaria un'ulteriore azione dell'Unione per attuare talune misure,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

1. La presente decisione si applica agli attacchi informatici con effetti significativi, inclusi tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.

2. Gli attacchi informatici che costituiscono una minaccia esterna includono quelli che:

a) provengono o sono sferrati dall'esterno dell'Unione;

b) impiegano infrastrutture esterne all'Unione;

c) sono compiuti da una persona fisica o giuridica, un'entità o un organismo stabiliti o operanti al di fuori dell'Unione; o

d) sono commessi con il sostegno, sotto la direzione o sotto il controllo di una persona fisica o giuridica, un'entità o un organismo operanti al di fuori dell'Unione.

3. A tal fine, gli attacchi informatici sono azioni che comportano:

a) accesso a sistemi di informazione;

b) interferenza in sistemi di informazione;

c) interferenza in dati; o

d) intercettazione di dati,

qualora tali azioni non siano debitamente autorizzate dal proprietario o da un altro titolare di diritti sul sistema o sui dati o su parte di essi ovvero non siano consentite a norma del diritto dell'Unione o dello Stato membro interessato.

4. Gli attacchi informatici che costituiscono una minaccia per gli Stati membri comprendono quelli che incidono su sistemi di informazione relativi, tra l'altro, a:

a) infrastrutture critiche, compresi i cavi sottomarini e gli oggetti lanciati nello spazio extratmosferico, essenziali per il mantenimento di funzioni vitali della società o della salute, dell'incolumità, della sicurezza e del benessere economico o sociale della popolazione;

b) servizi necessari per il mantenimento di attività sociali e/o economiche fondamentali, in particolare nei settori dell'energia (energia elettrica, petrolio e gas); trasporti (aerei, ferroviari, per idrovia e stradali); settore bancario; infrastrutture dei mercati finanziari; settore sanitario (prestatori di assistenza sanitaria, ospedali e cliniche private); fornitura e distribuzione di acqua potabile; infrastrutture digitali, e qualsiasi altro settore che sia essenziale per lo Stato membro interessato;

c) funzioni statali essenziali, in particolare nei settori della difesa, della governance e del funzionamento di istituzioni, anche per elezioni pubbliche o per la procedura elettorale, del funzionamento di infrastrutture economiche e civili, della sicurezza interna e delle relazioni esterne, anche attraverso missioni diplomatiche;

d) conservazione o trattamento di informazioni classificate; o

e) squadre di pronto intervento governative.

5. Gli attacchi informatici, che costituiscono una minaccia per l'Unione, comprendono quelli sferrati contro le sue istituzioni, i suoi organi e organismi, le sue delegazioni presso paesi terzi o organizzazioni internazionali, le sue operazioni e missioni di politica di sicurezza e di difesa comune (PSDC) e i suoi rappresentanti speciali.

6. Ove ritenuto necessario ai fini del conseguimento degli obiettivi della PESC enunciati nelle pertinenti disposizioni dell'articolo 21 del trattato sull'Unione europea, è possibile applicare misure restrittive a norma della presente decisione anche in risposta ad attacchi informatici con effetti significativi nei confronti di Stati terzi o organizzazioni internazionali.

Articolo 2

Ai fini della presente decisione si applicano le seguenti definizioni:

a) «sistemi di informazione»: dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali, nonché i dati digitali conservati, trattati, estratti o trasmessi da tale dispositivo o gruppo di dispositivi ai fini del loro funzionamento, del loro uso, della loro protezione e della loro manutenzione;

b) «interferenza in un sistema di informazione»: il fatto di ostacolare o interrompere il funzionamento di un sistema di informazione inserendo, trasmettendo, danneggiando, cancellando, deteriorando, alterando, sopprimendo o rendendo inaccessibili dati digitali;

c) «interferenza in dati»: il fatto di cancellare, danneggiare, deteriorare, alterare o sopprimere dati digitali contenuti in un sistema di informazione o di rendere tali dati inaccessibili; comprende inoltre il furto di dati, fondi, risorse economiche o proprietà intellettuale;

d) «intercettazione di dati»: il fatto di intercettare, tramite strumenti tecnici, trasmissioni non pubbliche di dati digitali verso, da o all'interno di un sistema di informazione, incluse le emissioni elettromagnetiche provenienti da un sistema di informazione contenente tali dati digitali.

Articolo 3

I fattori che determinano se un attacco informatico ha effetti significativi di cui all'articolo 1, paragrafo 1, comprendono:

a) portata, entità, impatto o gravità delle turbative causate, anche per quanto riguarda le attività economiche e sociali, i servizi essenziali, le funzioni statali essenziali, l'ordine pubblico o la sicurezza pubblica;

b) numero di persone fisiche o giuridiche, entità o organismi interessati;

c) numero di Stati membri interessati;

d) importo della perdita economica causata per esempio mediante furti su larga scala di fondi, risorse economiche o proprietà intellettuale;

e) vantaggio economico ottenuto dall'autore dell'atto per se stesso o per terzi;

f) quantità o natura dei dati oggetto del furto o entità delle violazioni dei dati; o

g) natura dei dati sensibili sotto il profilo commerciale cui si è avuto accesso.

Articolo 4

1. Gli Stati membri adottano le misure necessarie per impedire l'ingresso o il transito nello loro territorio di:

a) persone fisiche responsabili di attacchi informatici o tentati attacchi informatici;

b) persone fisiche che forniscono sostegno finanziario, tecnico o materiale per attacchi informatici o tentati attacchi informatici, o che sono altrimenti coinvolti in tali attacchi o tentati attacchi, anche pianificandoli, preparandoli, partecipandovi, dirigendoli, assistendoli o incoraggiandoli, oppure agevolandoli per azione o omissione;

c) persone fisiche associate a persone di cui alle lettere a) e b);

elencate nell'allegato.

2. Il paragrafo 1 non obbliga gli Stati membri a vietare ai loro cittadini l'ingresso nel proprio territorio.

3. Il paragrafo 1 lascia impregiudicate le situazioni in cui uno Stato membro sia vincolato da un obbligo derivante dal diritto internazionale, segnatamente:

a) in qualità di paese che ospita un'organizzazione intergovernativa internazionale;

b) in qualità di paese che ospita una conferenza internazionale convocata dalle Nazioni Unite o sotto gli auspici di questa organizzazione;

c) in virtù di un accordo multilaterale che conferisce privilegi e immunità; o

d) in virtù del trattato di conciliazione del 1929 (Patti Lateranensi) concluso tra la Santa Sede (Stato della Città del Vaticano) e l'Italia.

4. Il paragrafo 3 è considerato di applicazione anche qualora uno Stato membro ospiti l'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE).

5. Il Consiglio è debitamente informato in ciascuna delle situazioni in cui uno Stato membro concede una deroga a norma del paragrafo 3 o 4.

6. Gli Stati membri possono concedere deroghe alle misure stabilite a norma del paragrafo 1 allorquando il viaggio è giustificato da ragioni umanitarie urgenti o dall'esigenza di partecipare a riunioni intergovernative o a riunioni promosse o ospitate dall'Unione o ospitate da uno Stato membro che esercita la presidenza di turno dell'OSCE, in cui si conduce un dialogo politico che promuove direttamente gli obiettivi politici delle misure restrittive, compresa la sicurezza e la stabilità nel ciberspazio.

7. Gli Stati membri possono anche concedere deroghe alle misure stabilite a norma del paragrafo 1 quando l'ingresso o il transito è necessario per l'espletamento di un procedimento giudiziario.

8. Uno Stato membro che intenda concedere le deroghe di cui al paragrafo 6 o 7 presenta al riguardo una notifica scritta al Consiglio. La deroga si considera concessa a meno che, entro due giorni lavorativi dalla ricezione della notifica della deroga proposta, vi sia un'obiezione scritta di uno o più membri del Consiglio. Se uno o più membri del Consiglio sollevano obiezioni, il Consiglio, deliberando a maggioranza qualificata, può decidere di concedere la deroga proposta.

9. Qualora uno Stato membro autorizzi, a norma dei paragrafi 3, 4, 6, 7 o 8, l'ingresso o il transito nel suo territorio delle persone elencate nell'allegato, l'autorizzazione è strettamente limitata ai fini per i quali è concessa e alle persone direttamente interessate.

Articolo 5

1. Sono congelati tutti i fondi e le risorse economiche appartenenti a, posseduti, detenuti o controllati da:

a) persone fisiche o giuridiche, entità o organismi che sono responsabili di attacchi informatici o tentati attacchi informatici;

b) persone fisiche o giuridiche, entità o organismi che forniscono sostegno finanziario, tecnico o materiale per attacchi informatici o tentati attacchi informatici, o che sono altrimenti coinvolti in tali attacchi o tentati attacchi, anche pianificandoli, preparandoli, partecipandovi, dirigendoli, assistendoli o incoraggiandoli, oppure agevolandoli per azione o omissione;

c) persone fisiche o giuridiche, entità o organismi associati a persone fisiche o giuridiche, entità o organismi di cui alle lettere a) e b);

elencati nell'allegato.

2. Non sono messi a disposizione delle persone fisiche o giuridiche, delle entità e degli organismi elencati nell'allegato, direttamente o indirettamente, fondi o risorse economiche, né sono destinati a loro vantaggio.

3. In deroga ai paragrafi 1 e 2, le autorità competenti degli Stati membri possono autorizzare lo svincolo di taluni fondi o risorse economiche congelati o la messa a disposizione di taluni fondi o risorse economiche, alle condizioni che ritengono appropriate, dopo aver accertato che i fondi o le risorse economiche in questione sono:

a) necessari per soddisfare le esigenze di base delle persone fisiche elencate nell'allegato e dei familiari a loro carico, compresi i pagamenti relativi a generi alimentari, locazioni o ipoteche, medicinali e cure mediche, imposte, premi assicurativi e utenza di servizi pubblici;

b) destinati esclusivamente al pagamento di onorari ragionevoli o al rimborso delle spese sostenute per la prestazione di servizi legali;

c) destinati esclusivamente al pagamento di diritti o spese connessi alla normale gestione o alla custodia dei fondi o delle risorse economiche congelati;

d) necessari per coprire spese straordinarie, a condizione che la pertinente autorità competente abbia notificato alle autorità competenti degli altri Stati membri e alla Commissione, almeno due settimane prima dell'autorizzazione, i motivi per i quali ritiene che debba essere concessa una determinata autorizzazione; o

e) pagabili su o da un conto di una missione diplomatica o consolare o di un'organizzazione internazionale che gode di immunità in conformità del diritto internazionale, nella misura in cui tali pagamenti servono per scopi ufficiali della missione diplomatica o consolare o dell'organizzazione internazionale.

Lo Stato membro interessato informa gli altri Stati membri e la Commissione di ogni autorizzazione concessa ai sensi del presente paragrafo.

4. In deroga al paragrafo 1, le autorità competenti degli Stati membri possono autorizzare lo svincolo di taluni fondi o risorse economiche congelati a condizione che:

a) i fondi o le risorse economiche siano oggetto di una decisione arbitrale emessa anteriormente alla data dell'inserimento della persona fisica o giuridica, dell'entità o dell'organismo di cui al paragrafo 1 nell'elenco figurante nell'allegato, o siano oggetto di una decisione giudiziaria o amministrativa emessa nell'Unione, o di una decisione giudiziaria esecutiva nello Stato membro interessato, prima o dopo tale data;

b) i fondi o le risorse economiche siano usati esclusivamente per soddisfare i crediti garantiti da tale decisione o siano riconosciuti validi dalla stessa, entro i limiti fissati dalle leggi e dai regolamenti applicabili che disciplinano i diritti dei creditori;

c) la decisione non vada a favore di una persona fisica o giuridica, di un'entità o di un organismo elencati nell'allegato; e

d) il riconoscimento della decisione non sia contrario all'ordine pubblico dello Stato membro interessato.

Lo Stato membro interessato informa gli altri Stati membri e la Commissione di ogni autorizzazione concessa ai sensi del presente paragrafo.

5. Il paragrafo 1 non osta a che una persona fisica o giuridica, un'entità o un organismo elencati nell'allegato effettuino un pagamento dovuto nell'ambito di un contratto concluso prima della data in cui la persona fisica o giuridica, l'entità o l'organismo sono stati inseriti nell'allegato, purché lo Stato membro interessato abbia determinato che il pagamento non è percepito, direttamente o indirettamente, da una persona fisica o giuridica, da un'entità o da un organismo di cui al paragrafo 1.

6. Il paragrafo 2 non si applica al versamento sui conti congelati di:

a) interessi o altri profitti dovuti su detti conti;

b) pagamenti dovuti nel quadro di contratti, accordi o obblighi conclusi o sorti anteriormente alla data in cui tali conti sono stati assoggettati alle misure di cui ai paragrafi 1 e 2; o

c) pagamenti dovuti nel quadro di decisioni giudiziarie, amministrative o arbitrali emesse nell'Unione o esecutive nello Stato membro interessato,

purché tali interessi, altri profitti e pagamenti continuino a essere soggetti alle misure di cui al paragrafo 1.

Articolo 6

1. Il Consiglio, deliberando all'unanimità su proposta di uno Stato membro o dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, predispone e modifica l'elenco riportato nell'allegato.

2. Il Consiglio trasmette la decisione di cui al paragrafo 1, compresi i motivi dell'inserimento nell'elenco, alla persona fisica o giuridica, all'entità o all'organismo interessati direttamente, se l'indirizzo è noto, o mediante la pubblicazione di un avviso, offrendo a tale persona fisica o giuridica, entità o organismo la possibilità di presentare osservazioni.

3. Qualora siano presentate osservazioni o siano addotte nuove prove sostanziali, il Consiglio riesamina la decisione di cui al paragrafo 1 e ne informa di conseguenza la persona fisica o giuridica, l'entità o l'organismo interessati.

Articolo 7

1. L'allegato include i motivi dell'inserimento nell'elenco delle persone fisiche e giuridiche, delle entità e degli organismi di cui agli articoli 4 e 5.

2. Nell'allegato figurano, ove disponibili, le informazioni necessarie per identificare le persone fisiche o giuridiche, le entità o gli organismi interessati. Per le persone fisiche, tali informazioni possono includere: i nomi e gli pseudonimi; la data e il luogo di nascita; la cittadinanza; i numeri del passaporto e della carta d'identità; il sesso; l'indirizzo, se noto; e la funzione o professione. Per le persone giuridiche, le entità o gli organismi, tali informazioni possono comprendere le denominazioni, la data e il luogo di registrazione, il numero di registrazione e la sede di attività.

Articolo 8

Non è soddisfatta alcuna richiesta in relazione a contratti o operazioni sulla cui esecuzione hanno inciso, direttamente o indirettamente, integralmente o in parte, le misure istituite ai sensi della presente decisione, comprese richieste di indennizzo o richieste analoghe, per esempio richieste di compensazione o richieste nel quadro di una garanzia, in particolare richieste volte a ottenere la proroga o il pagamento di una garanzia o di una controgaranzia, in particolare di una garanzia o controgaranzia finanziaria, indipendentemente dalla sua forma, se la richiesta è presentata da:

a) persone fisiche o giuridiche, entità o organismi designati elencati nell'allegato;

b) qualsiasi persona fisica o giuridica, entità o organismo che agisca per tramite o per conto di una persona fisica o giuridica, un'entità o un organismo di cui alla lettera a).

Articolo 9

Per massimizzare l'impatto delle misure stabilite dalla presente decisione, l'Unione incoraggia i paesi terzi ad adottare misure restrittive analoghe a quelle previste nella presente decisione.

Articolo 10

La presente decisione si applica fino a 18 maggio 2020 ed è costantemente riesaminata. È prorogata o modificata, a seconda del caso, se il Consiglio ritiene che i suoi obiettivi non siano stati raggiunti.

Articolo 11

La presente decisione entra in vigore il giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Fatto a Bruxelles, il 17 maggio 2019

Per il Consiglio
Il presidente
E.O. TEODOROVICI

ALLEGATO

Elenco delle persone fisiche e giuridiche, delle entità e degli organismi di cui agli articoli 4 e 5

[…]