Ciberspazio. Il Consiglio Europeo rafforza la sicurezza contro gli attacchi informatici attraverso nuove misure restrittive

27/08/2019 PROTEZIONE DEI DATI E CYBERSECURITY, CONNETTIVITÀ, PROSPETTIVE

Roberto A. Jacchia
Marco Stillo

In data 17 maggio 2019, il Consiglio Europeo ha adottato la Decisione (PESC) 2019/797[1] ed il Regolamento (UE) n. 2019/796[2], istituendo un quadro normativo che consenta all'Unione Europea di imporre misure restrittive miranti a scoraggiare e contrastare gli attacchi informatici che costituiscono una minaccia esterna per l'UE o i suoi Stati membri.

Le nuove misure, che si applicano anche in caso di attacchi informatici nei confronti di Stati terzi o organizzazioni internazionali qualora ritenute necessarie per conseguire gli obiettivi della politica estera e di sicurezza comune (PESC), sono state fortemente volute da Olanda e Regno Unito in risposta all'attentato informatico contro l'Organizzazione per la proibizione delle armi chimiche (*Organisation for the Prohibition of*

[1] Decisione (PESC) 2019/797, del 17.05.2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, GUUE L 129I del 17.5.2019.
[2] Regolamento (UE) 2019/796 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, GUUE L 129I del 17.5.2019.

Chemical Weapons, OPAC) [3] sventato nell'ottobre 2018[4].

Il nuovo quadro normativo si inserisce nel solco dei recenti tentativi del Consiglio Europeo di proteggere l'integrità dell'Unione, dei suoi Stati membri e dei loro cittadini dalle minacce e dalle attività informatiche dolose intraprese da attori statali e non per il perseguimento dei propri obiettivi. A partire dall'adozione del pacchetto di strumenti della diplomazia informatica nel giugno 2017[5], infatti, il Consiglio ha più volte operato per migliorare il livello di sicurezza informatica degli Stati membri, da ultimo con l'adozione della Direttiva NIS[6] e del cosiddetto "*Cybersecurity Act*"[7].

A norma dell'articolo 1, paragrafo 3, della Decisione e del Regolamento, sono considerati attacchi informatici le azioni, non autorizzate dal proprietario o da altro titolare dei diritti sul sistema o sui dati, ovvero non consentite secondo la normativa dell'Unione europea o dello Stato membro interessato, che comportino accesso o interferenza ai sistemi di informazione oppure interferenza o intercettazione di dati[8]. Gli attacchi informatici devono rappresentare una minaccia esterna, ossia provenire dall'esterno dell'Unione o impiegare infrastrutture ad essa esterne, oppure essere compiuti direttamente o con il sostegno di soggetti, entità o organismi stabiliti o operanti al di fuori di essa[9].

Per rientrare nell'ambito di applicazione del nuovo quadro normativo è necessario che tali attacchi, perpetrati o anche solo tentati, producano degli effetti significativi o potenzialmente tali[10]. A tal proposito, né il Regolamento né la Decisione specificano in cosa questi "effetti significativi" consistano, salvo quanto

---

[3] L'OPAC è un'organizzazione internazionale, con sede all'Aia, che si occupa della promozione e della verifica del rispetto della convenzione sulle armi chimiche che ne vieta l'uso e ne chiede la distruzione.

[4] Per ulteriori informazioni, si veda il seguente LINK.

[5] Progetto di conclusioni del Consiglio, del 07.06.2017, su un quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose.

[6] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, GUUE L 194 del 19.7.2016.

[7] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013, *GUUE L 151 del 07.06.2019.*

[8] L'articolo 1 della Decisione 2019/797 e del Regolamento 2019/796 al paragrafo 3 così dispone: "*... 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,
se tali azioni non sono debitamente autorizzate dal proprietario o da un altro titolare di diritti sul sistema o sui dati o su parte di essi ovvero non sono consentite a norma del diritto dell'Unione o dello Stato membro interessato...".

[9] L'articolo 2 del Regolamento 2019/796 al paragrafo 2 così dispone: "*... 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...".

[10] L'articolo 1 del Regolamento 2019/796 al paragrafo 1 così dispone: "*... Il presente regolamento si applica agli attacchi informatici con effetti significativi, inclusi i tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri*".

disposto dall'articolo 3 di quest'ultima[11] che, al fine di verificarne la sussistenza, elenca una serie di fattori da tenere in considerazione, tra cui la portata, l'entità, l'impatto o la gravità delle turbative causate, il numero di persone fisiche o giuridiche interessate e la loro entità.

Per quanto riguarda le misure restrittive, la loro particolarità consiste nell'interessare tutti i soggetti in qualche modo collegati all'attacco informatico. Pertanto, non solo i diretti responsabili dell'azione (persone fisiche o organizzazioni), ma anche i loro finanziatori e coloro che li hanno assistiti a livello tecnico o materiale sono passibili di sanzione.

La prima sanzione[12] consiste nella possibilità per gli Stati Membri di adottare le misure che reputino necessarie per

[11] L'articolo 3 della Decisione 2019/797 così dispone: "*… 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…".

[12] L'articolo 4 della Decisione 2019/797 così dispone: "*… Gli Stati membri adottano le misure necessarie per impedire l'ingresso o il transito nel 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.
Il paragrafo 1 non obbliga gli Stati membri a vietare ai loro cittadini l'ingresso nel proprio territorio.
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.
Il paragrafo 3 è considerato di applicazione anche qualora uno Stato membro ospiti l'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE).
Il Consiglio è debitamente informato in ciascuna delle situazioni in cui uno Stato membro concede una deroga a norma del paragrafo 3 o 4.
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.
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.
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.

impedire l'ingresso o il transito all'interno del proprio territorio ai soggetti a qualsiasi titolo coinvolti in un attacco informatico, fatti salvi i casi in cui lo Stato sia tenuto a consentirne l'ingresso o la permanenza in base al diritto internazionale e alla possibilità di concedere delle deroghe. La seconda sanzione[13], invece, consiste nel congelamento di tutti i fondi e risorse

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…".

[13] L'articolo 5 della Decisione 2019/797 così dispone: "*… 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.

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.

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.

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. 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.

economiche riconducibili ai soggetti a qualsiasi titolo coinvolti in un attacco informatico, e nell'impossibilità di mettere tali risorse a loro disposizione sia direttamente che indirettamente. Anche in questo caso, gli Stati membri possono concedere delle deroghe, autorizzando lo svincolo di alcuni fondi o risorse economiche o la loro messa a disposizione.

Il nuovo quadro normativo conferma l'impegno assunto dall'Unione nel mantenere un ciberspazio aperto, sicuro e rispettoso delle libertà fondamentali, in cui le controversie possano essere pacificamente risolte attraverso una maggiore cooperazione internazionale. L'articolo 9 della Decisione[14], che invita i Paesi terzi ad adottare misure restrittive analoghe, riprende, infatti, le dichiarazioni dell'Alta Rappresentante a nome dell'UE, secondo cui "... [l]*'Unione europea e i suoi Stati membri esortano gli attori a porre fine alle attività dolose e invitano tutti i partner a rafforzare la cooperazione internazionale per promuovere la sicurezza e la stabilità nel ciberspazio...*"[15].

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…".

[14] L'articolo 9 della Decisione 2019/797 così dispone: "*… 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…*".

[15] Per ulteriori informazioni, si veda il seguente LINK.

Roberto A. Jacchia
PARTNER

r.jacchia@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 - Milano

Marco Stillo
ASSOCIATE

m.stillo@dejalex.com
+32 (0)26455670
Chaussée de La Hulpe 187
1170 - Bruxelles

MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Ulitsa Bolshaya Ordynka 37/4 · 119017, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com