DIRITTO PENALE CONTEMPORANEO

DIRITTO PENALE CONTEMPORANEO

Fascicolo
1/2019

ISSN 2039-1676

Diritto Penale Contemporaneo è un periodico on line, ad accesso libero e senza fine di profitto, nato da un'iniziativa comune di Luca Santa Maria, che ha ideato e finanziato l'iniziativa, e di Francesco Viganò, che ne è stato sin dalle origini il direttore nell'ambito di una partnership che ha coinvolto i docenti, ricercatori e giovani cultori della Sezione di Scienze penalistiche del Dipartimento "C. Beccaria" dell'Università degli Studi di Milano. Attualmente la rivista è edita dall'Associazione "Diritto penale contemporaneo", il cui presidente è l'Avv. Santa Maria e il cui direttore scientifico è il Prof. Gian Luigi Gatta. La direzione, la redazione e il comitato scientifico della rivista coinvolgono oggi docenti e ricercatori di numerose altre università italiane e straniere, nonché autorevoli magistrati ed esponenti del foro.
Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Comittee on Publication Ethics).

***Peer review*.**
Salvo che sia diversamente indicato, tutti i contributi pubblicati nella sezione *papers* di questo fascicolo hanno superato una procedura di *peer review*, attuata secondo principi di trasparenza, autonomia e indiscusso prestigio scientifico dei revisori, individuati secondo criteri di competenza tematica e di rotazione all'interno dei membri del Comitato scientifico. Ciascun lavoro soggetto alla procedura viene esaminato in forma anonima da un revisore, il quale esprime il suo parere in forma parimenti anonima sulla conformità del lavoro agli standard qualitativi delle migliori riviste di settore. La pubblicazione del lavoro presuppone il parere favorevole del revisore. Di tutte le operazioni compiute nella procedura di *peer review* è conservata idonea documentazione presso la redazione.

Modalità di citazione.
Per la citazione dei contributi presenti nei fascicoli di *Diritto penale contemporaneo*, si consiglia di utilizzare la forma di seguito esemplificata: N. COGNOME, *Titolo del contributo*, in *Dir. pen. cont.*, fasc. 1/2017, p. 5 ss.

1/2019

ACCESSO TRANSNAZIONALE ALLA PROVA ELETTRONICA NEL PROCEDIMENTO PENALE: LA NUOVA INIZIATIVA LEGISLATIVA DELLA COMMISSIONE EUROPEA AL VAGLIO DEL CONSIGLIO DELL'UNIONE

di Raffaella Pezzuto

SOMMARIO: 1. Le iniziative legislative presentate dalla Commissione europea il 17 aprile 2018 per agevolare l'acquisizione transnazionale e la conservazione delle prove elettroniche in materia penale (*e-evidence*). *Ratio legis*. – 2. La proposta di Direttiva sulla nomina di rappresentanti legali da parte dei prestatori di servizi ai fini dell'acquisizione di prove nei procedimenti penali (COM(2018)226 final). – 3. La proposta di Regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (COM(2018)225 final) alla luce dell'orientamento generale del Consiglio dell'Unione europea del 7 dicembre 2018 (ST15292/18). – 3.1. Il rapporto con l'ordine europeo di indagine penale. – 3.2. Autorità nazionali competenti ad emettere gli ordini europei di produzione e di conservazione della prova elettronica. – 3.3. Definizione di "prova elettronica". Esclusione delle intercettazioni in tempo reale. Il problema dei dati criptati. – 3.4. I procedimenti nazionali in cui possono essere emessi gli ordini europei di produzione e di conservazione della prova elettronica. Il principio di specialità. – 3.5. I presupposti per l'emissione dell'ordine europeo di produzione della prova elettronica e il meccanismo di notifica allo Stato di esecuzione. – 3.6. I presupposti per l'emissione dell'ordine europeo di conservazione della prova elettronica. – 3.7. Il destinatario degli ordini europei relativi alla prova elettronica e i certificati di ordine europeo di produzione (EPOC) e di ordine europeo di conservazione (EPOC-PR). – 3.8. La procedura di riesame in caso di conflitto dell'ordine di produzione con la legislazione di un paese terzo. Il mandato alla Commissione europea a negoziare un accordo con gli Stati Uniti. – 4. Conclusioni.

1. Le iniziative legislative presentate dalla Commissione europea il 17 aprile 2018 per agevolare l'acquisizione transnazionale e la conservazione delle prove elettroniche in materia penale (*e-evidence*). *Ratio legis*.

Dopo gli attentati terroristici di Bruxelles del 2016, gli Stati membri hanno sottolineato in varie occasioni l'urgenza di individuare modalità per assicurare ed ottenere più rapidamente ed efficacemente prove digitali nell'ambito dei procedimenti penali, intensificando la cooperazione con i paesi terzi e con i prestatori di servizi internet, al fine di adottare misure omogenee a livello UE per difendere lo stato di diritto nel cyberspazio[1].

[1] Vedasi la Dichiarazione comune dei Ministri della Giustizia e degli Interni dell'UE e dei rappresentanti delle Istituzioni UE sugli attentati terroristici di Bruxelles del 22 marzo 2016 e le Conclusioni del Consiglio dell'Unione europea sul miglioramento della giustizia penale nel cyberspazio del 9 giugno 2016 (ST9579/16). Cfr. sul tema G. SUFFIA, *Geografia delle cyberwars. Uomini e Stati alla prova dello spazio digitale*, Milano, 2018.

Nella medesima direzione, i co-legislatori europei, nella Direttiva (UE) 2017/541, hanno statuito, nel considerando n. 7, che il carattere transnazionale del fenomeno terroristico richiede una risposta globale e impone quindi il rafforzamento della cooperazione da parte dell'Unione europea e dei suoi Stati membri con il resto del mondo, proponendo altresì l'adozione di strumenti di collaborazione con i paesi terzi finalizzati anche alla raccolta e all'ottenimento di prove elettroniche[2].

Recependo queste indicazioni, il 17 aprile 2018 la Commissione europea ha presentato un pacchetto di misure in materia di lotta al terrorismo tra cui una proposta di Regolamento finalizzato a migliorare l'accesso transnazionale alle prove elettroniche attraverso l'introduzione degli ordini europei di produzione e di conservazione della prova elettronica (*e-evidence*) in ambito penale e una proposta di Direttiva che individua regole comuni sulla designazione dei legali rappresentanti dei *providers* per facilitare l'accesso alle prove elettroniche detenute dai fornitori di servizi con sede legale in un Paese europeo diverso da quello dell'autorità giudiziaria richiedente. Tali misure, ove adottate, consentiranno di potenziare significativamente i mezzi investigativi di prevenzione e contrasto del terrorismo e della radicalizzazione violenta, anche con riferimento alla propaganda e al reclutamento a fini terroristici attraverso il web.

Prima di passare ad analizzare le novità contenute nelle iniziative legislative in parola, giova innanzitutto descrivere brevemente quali sono gli aspetti critici dell'attuale quadro normativo che la Commissione europea ha tentato di affrontare. L'attuale quadro normativo dell'Unione contempla già strumenti di cooperazione giudiziaria internazionale atti a consentire l'acquisizione transfrontaliera delle prove elettroniche nei procedimenti penali, basati su meccanismi di riconoscimento reciproco nei rapporti tra Stati membri e sull'assistenza giudiziaria nei rapporti con i paesi terzi. Tra i principali ricordiamo la Direttiva 2014/41/UE sull'ordine europeo di indagine penale (EIO)[3]; la Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea del 29 maggio 2000[4]; il Regolamento (UE) 2018/1727 del 14

---

[2] S. SANTINI, *L'Unione europea compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della Direttiva 2017/541*, in questa *Rivista*, fascicolo 7-8/2017, p. 13 ss.; S. DE LUCA, *La direttiva 2017/541/UE e il difficile bilanciamento tra esigenze di pubblica sicurezza e rispetto dei diritti umani*, in *Eurojus*, 3 luglio 2017; con riferimento alla trasposizione della Direttiva 2017/541 nel nostro ordinamento, vedasi la scheda del Servizio Studi della Camera dei Deputati e del Senato, alle pagine 191 ss., sulla delega al Governo per il relativo recepimento nella Legge di delegazione europea 2016/2017 (L. 25 ottobre 2017, n. 163).

[3] Per una compiuta analisi dei principi informatori della Direttiva 2014/41/UE, si rinvia ai primi commenti di R. BELFIORE, *Riflessioni a margine della direttiva sull'ordine europeo di indagine penale*, in *Cassazione penale*, 2015, p. 3288C, fasc. 9; L. CAMALDO – F. CERQUA, *La direttiva sull'ordine europeo di indagine penale. Le nuove prospettive per la libera circolazione delle prove*, in *Cassazione penale*, 10/2014, p. 3511B. Sugli aspetti inerenti all'entrata a regime dell'ordine europeo di indagine penale nel nostro ordinamento, vedasi M. DANIELE, *L'ordine europeo di indagine penale entra a regime. Prime riflessioni sul d.lgs. n. 108 del 2017*, in questa *Rivista*, fasc. 7-8/2017, p. 208 ss.; E. SELVAGGI, *La Circolare del Ministero della Giustizia sul c.d. ordine europeo di indagine*, in questa *Rivista*, fasc. 11/2017, p. 287 ss.; A. NOCERA, *Il sindacato giurisdizionale interno in tema di ordine europeo di intercettazione*, in questa *Rivista*, fasc. 1/2018, p. 149 ss.

[4] Sul recepimento della Convenzione di Bruxelles del 2000 nel nostro ordinamento attraverso il d.lgs. 5 aprile 2017, n. 52, vedasi L. CAMALDO, *L'attuazione della Convenzione di Bruxelles del 2000: l'assistenza giudiziaria in materia penale assume una configurazione a "geografia variabile"*, in questa *Rivista*, fasc. 7-8/2017, p. 202 ss.; S. MONICI, *Emanate le norme di attuazione della Convenzione di assistenza giudiziaria in materia penale del 29 maggio*

novembre 2018 che istituisce *Eurojust* (e abroga la precedente Decisione 2002/187/GAI del Consiglio); il Regolamento (UE) 2016/794 che istituisce *Europol*; la Decisione quadro 2002/465/GAI del Consiglio relativa alle squadre investigative comuni[5]; gli accordi bilaterali sulla mutua assistenza giudiziaria tra l'Unione e gli Stati terzi, come quello con gli Stati Uniti d'America[6] e con il Giappone[7].

Nella pratica operativa, tuttavia, l'acquisizione di prove digitali ha incontrato alcune peculiari criticità che il pur articolato ed ampio strumentario normativo appena ricordato tuttora non consente di affrontare efficacemente. In particolare, uno dei maggiori ostacoli all'ottenimento dell'*e-evidence* risiede nel fatto che i fornitori di servizi telematici non hanno, allo stato, alcun obbligo generale di essere fisicamente presenti nel territorio dell'Unione, potendo offrire i propri servizi in linea di massima da qualsiasi luogo del mondo, senza necessità di infrastrutture, di aziende o personale presente negli Stati membri. Spesso accade, pertanto, che rifiutino la produzione della prova digitale deducendo la carenza di giurisdizione dell'autorità procedente in ragione ora del luogo di stabilimento della propria sede principale, ora del luogo di ubicazione (*"storage"*) dei dati, ora della cittadinanza della persona in relazione alla quale questi ultimi sono stati richiesti (*"affected person"*). Il quadro si complica ulteriormente quando nel caso concreto ricorrano profili di collegamento con l'ordinamento di paesi terzi, eventualità particolarmente ricorrente giacché molti dei maggiori fornitori di servizi telematici hanno sede legale negli Stati Uniti.

Inoltre, l'acquisizione di prove elettroniche mediante procedure di cooperazione giudiziaria, tradizionale o fondata sul mutuo riconoscimento, ha evidenziato profili di criticità legati al necessario coinvolgimento dell'autorità (giudiziaria o governativa) dello Stato di esecuzione, che implica un'inevitabile dilatazione dei tempi, incompatibile con la "volatilità" del dato elettronico.

Le difficoltà in parola sono state riscontrate non solo nell'applicazione degli strumenti di cooperazione giudiziaria dell'Unione europea sopra indicati, ma anche di quelli del Consiglio d'Europa ed in particolare della Convenzione di Budapest del 23 novembre 2001 sulla criminalità informatica, ratificata al momento da sessantadue Paesi, tra cui tutti gli Stati membri dell'Unione europea ad eccezione dell'Irlanda e della Svezia, nonché da molti Paesi terzi non appartenenti al Consiglio d'Europa tra cui gli Stati Uniti,

---

2000: quali margini operativi in vista dell'(imminente) trasposizione della direttiva sull'ordine europeo di indagine penale, in *Eurojus*, 3 maggio 2017; E. SELVAGGI, *Un ammodernamento diventato necessario per tutti gli Stati UE*, in *Guida dir.*, 2017, n. 25, p. 45 ss.

[5] E. GONZATO, *Squadre investigative comuni: l'Italia finalmente recepisce la decisione quadro 2002/465/GAI*, in *Eurojus*, 14 marzo 2016; G. COLAIACOVO, *Nuove prospettive in tema di coordinamento delle indagini e cooperazione giudiziaria alla luce della disciplina delle squadre investigative comuni*, in *Dir. pen. cont. – Riv. trim.*, 1/2017, p. 169 ss.

[6] Decisione 2009/820/PESC del Consiglio del 23 ottobre 2009, relativa alla conclusione, a nome dell'Unione europea, dell'accordo sull'estradizione tra l'Unione europea e gli Stati Uniti d'America e dell'accordo sulla mutua assistenza giudiziaria tra l'Unione europea e gli Stati Uniti d'America.

[7] Decisione 2010/616/UE del Consiglio del 7 ottobre 2010, relativa alla conclusione dell'accordo tra l'Unione europea e il Giappone sull'assistenza giudiziaria reciproca in materia penale.

il Canada, l'Australia, Israele, l'Argentina, il Cile e il Giappone[8]. Tale Convenzione, invero, già prevede, agli articoli da 16 a 18, precisi obblighi a carico degli Stati Parte di istituire nei loro ordinamenti interni ingiunzioni di produzione per ottenere dati informatici da prestatori di servizi presenti sul proprio territorio e dati relativi agli abbonati da prestatori di servizi che offrono servizi sul proprio territorio; prevede, altresì, la possibilità di ordinare la conservazione di dati informatici, soprattutto qualora sussistano motivi per ritenere che gli stessi siano particolarmente a rischio di perdita o modificazione. Tuttavia, la notificazione e l'esecutività delle ingiunzioni nazionali di produzione emessi ai sensi della Convenzione in parola ha incontrato notevoli difficoltà nel caso in cui fossero indirizzate a prestatori di servizi stabiliti al di fuori del territorio dello Stato Parte richiedente, tanto che il Consiglio d'Europa sta attualmente lavorando all'adozione di un Secondo Protocollo addizionale alla Convenzione di Budapest che migliori l'accesso transfrontaliero alle prove elettroniche rendendolo indipendentemente dal luogo di conservazione dei dati[9]. Tali lavori stanno procedendo nella piena consapevolezza della necessità che l'adottando strumento sia del tutto coerente con le proposte normative attualmente in fase di negoziato a livello UE in materia di *e-evidence*, considerato che tutti gli Stati membri dell'UE fanno parte anche del Consiglio d'Europa e che non potrebbero, pertanto, assumere obblighi normativi internazionali tra loro disomogenei o confliggenti [10].

---

[8] Sulla ratifica della Convenzione di Budapest del 2001 sulla criminalità informatica nel nostro ordinamento, avvenuta con legge 18 marzo 2008, n. 48, vedasi G. CORASANITI, G. CORRIAS LUCENTE, *Cybercrime, responsabilità degli enti, prova digitale*, Padova, 2009; L. LUPARIA (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime (l. 18 marzo 2008, n. 48)*, Milano, 2009; sulla ricerca e raccolta della prova digitale, L. BARTOLI, C. MAIOLI, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, in *Informatica e diritto*, Vol. XXIV, 2015, n. 1-2, p. 139 ss.

[9] La Commissione per la Convenzione sulla criminalità informatica del Consiglio d'Europa (T-CY) ha adottato, nella sua 17ª sessione di lavori del 7 giugno 2017, il mandato per la preparazione di un Secondo protocollo addizionale alla Convenzione di Budapest, che dovrebbe essere ultimato dalla TC-Y entro dicembre 2019, indicando gli aspetti dell'attuale Convenzione che dovrebbero essere migliorati (vedansi al riguardo i *Terms of reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime* del 7 giugno 2017, accessibili a questo *link*. Si segnala, inoltre, che il sito del Consiglio d'Europa pubblica costanti informazioni di aggiornamento sullo stato dei lavori al seguente *link*.

[10] Sulla necessità di coerenza tra i due strumenti normativi, vedasi il rapporto della Terza Sessione plenaria del TC-Y tenutasi il 28-29 novembre 2018 a Strasburgo, a questo *link*. Appare, inoltre, importante evidenziare che la Commissione europea sta seguendo con grande attenzione le attività del Consiglio d'Europa di stesura del Secondo Protocollo addizionale alla Convenzione di Budapest, come risulta dalla Comunicazione dalla stessa indirizzata al Parlamento europeo, al Consiglio europeo e al Consiglio UE in data 10 ottobre 2018, dal titolo "Sedicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della Sicurezza" (COM(2018) 690 final), in cui viene esplicitata l'importanza di un approccio coerente e coordinato da parte dell'UE rispetto al tema della *e-evidence* non solo all'interno dello spazio unico di libertà, giustizia e sicurezza, ma anche da parte dell'UE a livello internazionale, con particolare riferimento ai negoziati in corso in seno al Consiglio d'Europa. Nel citato documento si evidenzia che la Commissione europea intende proporre al più presto l'adozione di una raccomandazione per ricevere dal Consiglio direttive di negoziato sul Secondo Protocollo addizionale alla Convenzione di Budapest, conformemente a quanto richiesto dal Consiglio stesso nel giugno 2018 (vedasi p. 12).

A causa delle segnalate criticità degli strumenti convenzionali internazionali, taluni Stati membri hanno recentemente adottato misure, a livello nazionale, finalizzate ad assicurare l'accesso a prove digitali o ad altri tipi di informazioni che possano essere utili nell'ambito di procedimenti penali, scegliendo tuttavia approcci diversi tra loro, che vanno dall'ampliamento della competenza delle autorità giudiziarie ad intraprendere un atto di indagine, all'obbligo per i *service providers* di designare un rappresentante legale nel territorio dello Stato membro in cui offre i propri servizi.[11] Questo ha portato ad una frammentazione delle normative nazionali nel territorio dell'Unione non solo per quanto attiene alle regole applicabili per stabilire la giurisdizione di ciascuno Stato membro sul prestatore di servizi (le discipline nazionali variano, ad esempio, a seconda che tale giurisdizione venga ancorata alla sede principale dell'impresa o al luogo in cui sono offerti i servizi o all'ubicazione dei dati o a una combinazione di questi fattori), ma anche alla obbligatorietà o meno per il prestatore di servizi di ottemperare alle richieste provenienti dalle autorità giudiziarie degli Stati membri, con conseguente diversità di regimi applicabili in materia di misure sanzionatorie in caso di inottemperanza. La necessità di adempiere ad obblighi giuridici nazionali differenti (e talvolta addirittura

---

[11] Ad esempio, la Germania ha approvato nel 2017 una legge per migliorare l'applicazione del diritto nei *social network* in base alla quale i *providers* sono obbligati a designare una persona in Germania abilitata a ricevere richieste di informazioni dalle autorità di contrasto (*link*). La legge prevede sanzioni fino a 500.000 euro in caso di mancata nomina di rappresentante legale o di mancata risposta a richieste di informazioni da parte della persona abilitata a riceverle. Altri Stati membri, come il Belgio, non richiedono una rappresentanza locale ma cercano piuttosto di far valere gli obblighi nazionali direttamente nei confronti dei prestatori di servizi stabiliti all'estero mediante procedimenti nazionali. Il dibattito si è aperto anche in Italia, dove la questione è stata affrontata anche con riferimento alla legittimità dell'utilizzo dei captatori informatici: si ricorda in particolare la relazione annuale della Direzione Nazionale Antimafia e Antiterrorismo sulle attività svolte, nonché sulle dinamiche e strategie della criminalità organizzata di tipo mafioso relativa al periodo 1° luglio 2014 – 30 giugno 2015 (*link*), dove si individuano le persistenti criticità nella ricerca delle evidenze elettroniche: *"Problemi irrisolti nella conservazione ed acquisizione dei dati. Si constata nella pratica che molti Stati non dispongono di un quadro giuridico adeguato, in materia di prove digitali. Le perquisizioni dei computer sono spesso effettuate nell'ambito delle norme generali relative alla perquisizione e al sequestro, che non sono sempre adeguate, come ad esempio per l'accesso a distanza a reti di computer. L'accesso remoto all'hard disk di un computer grazie all'utilizzo di cavalli di Troia (Trojan) o altri programmi di pirateria informatica suscita ampi dibattiti, poiché può essere realizzato al di là delle frontiere, solleva questioni di competenza e di sovranità nazionali. L'assenza di una normativa completa e/o le differenze tra le legislazioni degli Stati aumentano naturalmente le difficoltà della cooperazione transnazionale e il trasferimento delle prove"* (vedasi pag. 197). Anche la dottrina si è occupata del tema: vedasi, per una ricostruzione sistemica, il recente contributo di S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Padova, 2018; per una panoramica sui potenziali usi processuali del captatore informatico alla luce delle sue caratteristiche tecniche, R. BRIGHI, *Funzionamento e potenzialità investigative del malware*, in *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di G. Giostra e R. Orlandi, Torino, 2018, p. 221 ss.; M. BONTEMPELLI, *Il captatore informatico in attesa della riforma*, in questa *Rivista*, 20 dicembre 2018, che analizza le novità introdotte dalla "riforma Orlando" (d.lgs. n. 2016/2017) sulle condizioni e i limiti di utilizzabilità processuale dell'intercettazione tramite captatore informatico. Quanto alla giurisprudenza di legittimità sul tema, si segnala l'orientamento della Suprema Corte (vedasi, tra le altre, Cass. pen., sent. n. 46968/2017 e sent. n. 50452/2015) secondo cui sono da considerarsi prove ammissibili le *chat* acquisite tramite dispositivi Blackberry "*pin to pin*" in assenza di rogatoria internazionale qualora le comunicazioni siano avvenute in Italia, a nulla rilevando che per decriptare i dati identificativi associati ai codici "*pin*" sia necessario ricorrere alla collaborazione del produttore del sistema operativo avente sede all'estero.

tra loro confliggenti) ha, peraltro, determinato per i *service providers* un notevole aumento dei costi amministrativi, che si sono rivelati particolarmente gravosi per le imprese di minori dimensioni, così creando ostacoli alla prestazione dei servizi e al corretto funzionamento del mercato unico europeo.

Al fine di superare questi problemi e di rendere più efficienti le procedure di acquisizione e di conservazione delle prove nell'ambito dei procedimenti penali, soprattutto con riferimento a quelle digitali, il 17 aprile 2018 la Commissione europea ha presentato due proposte normative tra loro complementari:

– una proposta di Direttiva del Parlamento europeo e del Consiglio recante norme armonizzate sulla nomina di rappresentanti legali da parte dei prestatori di servizi ai fini dell'acquisizione di prove nei procedimenti penali (COM(2018)226 final);

– una proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (COM(2018)225 final)[12].

Con il primo strumento si mira ad armonizzare le regole sulla rappresentanza legale di alcuni prestatori di servizi all'interno dell'Unione, al fine di identificare chiaramente a chi le autorità competenti degli Stati membri possano indirizzare i propri provvedimenti di acquisizione della prova emessi nei procedimenti penali e secondo quali procedure, così prevedendo una soluzione comune atta a superare l'attuale frammentazione delle discipline nazionali e a facilitare l'ottemperanza da parte dei *service providers*. Con il secondo, invece, si persegue l'obiettivo di notificare direttamente gli ordini europei di produzione e di conservazione di prove elettroniche al prestatore di servizi nei casi in cui le autorità nazionali competenti rivolgano tali ordini a *providers* che non siano stabiliti sul proprio territorio.

Giova da subito menzionare che il negoziato sulle due proposte normative è stato avviato nell'ambito del gruppo di lavoro COPEN (*Working party on Cooperation in Criminal matters*) del Consiglio dell'Unione europea il 27 aprile 2018 sotto Presidenza bulgara ed è poi proseguito sotto Presidenza austriaca nel secondo semestre del 2018. Gli sforzi delle delegazioni si sono finora concentrati sulla proposta di Regolamento in merito alla quale il Consiglio UE – nella composizione Giustizia e Affari interni - ha raggiunto l'orientamento generale il 7 dicembre 2018, consentendo così l'avvio del negoziato di trilogo tra Commissione europea, Consiglio UE e Parlamento europeo, con l'auspicio che lo strumento possa essere definitivamente adottato prima delle elezioni parlamentari europee di maggio 2019. Nessun orientamento generale è stato, invece, ancora adottato dal Consiglio UE sulla proposta di Direttiva, che continuerà ad essere discussa dagli Stati membri in sede COPEN, sotto la Presidenza rumena del primo semestre 2019.

Pertanto, nel presente studio si prenderanno in considerazione il testo dell'orientamento generale adottato dal Consiglio UE – Giustizia e Affari interni il 7 dicembre 2018 in relazione alla proposta di Regolamento relativo agli ordini europei di

---

[12] Cfr. sul tema M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in questa *Rivista*, fasc. 5/2018, p. 277 ss.

produzione e di conservazione di prove elettroniche in materia penale (ST15292/18 del 12 dicembre 2018)[13] e il testo della proposta di Direttiva presentato dalla Commissione europea il 17 aprile 2018 (COM(2018)226 final)[14], tentando di evidenziare gli aspetti di quest'ultima che fin da ora appaiono suscettibili di modifiche nel prosieguo del negoziato in considerazione dell'orientamento generale raggiunto dal Consiglio UE sulla proposta di Regolamento.

2. La proposta di Direttiva sulla nomina di rappresentanti legali da parte dei prestatori di servizi ai fini dell'acquisizione di prove nei procedimenti penali (COM(2018)226 final).

La proposta di Direttiva in parola mira a stabilire un obbligo per il prestatore che offra i propri servizi nel territorio dell'Unione di designare almeno un rappresentante legale nell'UE, ovvero una persona fisica o giuridica che agisca in suo nome e per suo conto al fine di ottemperare ai provvedimenti (decisioni e ordini) emessi dalle autorità nazionali competenti per acquisire prove nell'ambito di procedimenti penali pendenti negli Stati membri[15].

Rientrano nel campo di applicazione della proposta di Direttiva i seguenti tipi di prestatori di servizi: prestatori di servizi di comunicazione elettronica, prestatori di servizi della società dell'informazione che conservano dati nell'ambito dei servizi prestati agli utenti, comprese reti sociali, mercati online e altri prestatori di servizi di hosting e prestatori di nomi e servizi di numerazione per internet (vedasi articolo 2 della proposta di Direttiva). Essi devono avere un "collegamento sostanziale" con l'Unione, che sicuramente esiste quando il *service provider* ha uno stabilimento nel territorio dell'Unione. In mancanza di questo, il criterio del collegamento sostanziale con l'Unione dovrebbe essere valutato sulla base dell'esistenza di un numero significativo di utenti in uno o più Stati membri, o della destinazione delle attività verso uno o più Stati membri deducibile, per esempio, dall'uso di una lingua o di una moneta generalmente utilizzata nello Stato membro in questione o la possibilità di ordinare prodotti o servizi. La semplice accessibilità del servizio, invece, non dovrebbe di per sé costituire condizione

[13] Testo accessibile a questo *link*.
[14] Testo accessibile a questo *link*.
[15] L'obbligo di designare un rappresentante legale per i prestatori di servizi non stabiliti nell'UE ma che offrono servizi nell'UE è già previsto da altri strumenti normativi dell'Unione quali, ad esempio, il regolamento generale sulla protezione dei dati (UE) 2016/679 (vedasi articolo 27) e la direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (vedasi articolo 18). E', inoltre, previsto nella proposta della Commissione (COM(2017)10 final), ancora in fase di negoziato a livello UE, finalizzata all'adozione di un regolamento sulla e-Privacy (vedasi articolo 3) che sostituisca la direttiva 2002/58/CE (vedasi al riguardo T. WESSING, *Where is the e-Privacy Regulation?*, 28 novembre 2018, accessibile a questo *link*). Nulla esclude che il rappresentante legale designato da un'impresa nel territorio dell'UE possa svolgere cumulativamente tutte le funzioni previste dai menzionati strumenti UE in materia di protezione dei dati personali e quelle contemplate dalla proposta di Direttiva in esame, relativa all'acquisizione di prove nei procedimenti penali (vedasi, in tal senso, pag. 5 della proposta di Direttiva).

sufficiente per l'applicazione della direttiva (vedasi considerando 12 e 13 della proposta di Direttiva).

Giova menzionare che la medesima definizione di prestatore che offre servizi nell'Unione è contenuta nella proposta di Regolamento relativo agli ordini europei di produzione e di conservazione delle prove elettroniche in materia penale, precisamente all'articolo 2(3) e 2(4). Tuttavia, il testo dell'orientamento generale sulla proposta di Regolamento adottato il 7 dicembre 2018 presenta delle modifiche alla definizione in parola, finalizzate a: escluderne dall'ambito di applicazione i prestatori di servizi finanziari di cui all'articolo 2(2)(b) della Direttiva 2006/123/CE; chiarire a quali prestatori di servizi della società dell'informazione (definiti dalla Direttiva 2015/1535/UE) si applica il nuovo Regolamento; a precisare che il collegamento sostanziale con l'Unione deve basarsi su "specifici criteri fattuali". Attesa la simmetria tra i due strumenti normativi e la conseguente esigenza di coerenza intrinseca, è prevedibile che l'attuale formulazione dell'articolo 2(2) e 2(3) della proposta di Direttiva verrà modificata nel corso del negoziato al fine di rispecchiare il testo definitivo dell'articolo 2(3) e 2(4) della proposta di Regolamento.

Vale, inoltre, precisare che – ai sensi dell'articolo 1(4) - è escluso dall'ambito di applicazione della proposta di Direttiva il prestatore di servizi stabilito sul territorio di uno Stato membro che offra i propri servizi solo su quel territorio.

Per quanto attiene alle prove a cui la proposta di Direttiva si riferisce, l'articolo 1 prevede, con formulazione ampia, che si tratta dell'acquisizione di prove nei procedimenti penali. Se ne deduce che esse possono essere di natura elettronica (*e-evidence*) o di altra tipologia: si segnala al riguardo che la definizione di "prova elettronica" è contenuta nell'articolo 2(6) della proposta di Regolamento relativo agli ordini europei di produzione e di conservazione delle prove elettroniche in materia penale, secondo cui è "elettronica" la prova che sia conservata in formato elettronico da un prestatore di servizi o per suo conto *al momento della ricezione* del certificato di ordine europeo di produzione o conservazione (di cui parleremo in seguito) e consiste nei *dati conservati relativi agli abbonati, agli accessi, alle operazioni o al contenuto*.

In linea di principio, il *service provider* può decidere liberamente in quale Stato membro designare il proprio rappresentante legale purché sia uno Stato membro in cui fornisce servizi o ha la propria sede di stabilimento: ciò al fine di evitare che la scelta si diriga verso un Paese con cui il *provider* non ha nessuna connessione, magari solo per ragioni inerenti all'importo delle sanzioni che – ai sensi dell'articolo 5 della proposta di Direttiva – potranno essere comminate a suo carico in caso di violazione delle disposizioni nazionali adottate in via di recepimento della Direttiva stessa, il cui importo potrà essere diverso a seconda degli Stati membri[16]. Nel caso in cui l'internet service provider abbia una o più sedi europee di stabilimento secondo la definizione fissata nell'articolo 2 (4) della proposta di Direttiva, l'obbligo di designazione di un legale

[16] L'articolo 5 della Proposta di Direttiva prevede, infatti, che siano gli Stati membri a stabilire autonomamente le sanzioni da irrogare ai *providers* in caso di violazione delle disposizioni nazionali adottate ai sensi della Direttiva, senza fissare dunque sanzioni armonizzate a livello UE ma prevedendo solo che gli Stati membri le determinino in maniera tale che siano efficaci, proporzionate e dissuasive.

rappresentante deve essere imposto dallo Stato membro o dagli Stati membri in cui il prestatore di servizi è stabilito. Ove, invece, il *provider* non sia stabilito nell'Unione, l'imposizione di questo obbligo spetta agli Stati membri in cui i servizi vengono prestati.

Al riguardo è bene precisare che, come regola generale, i *service providers* non possono essere obbligati a designare nell'Unione più di un rappresentante legale, né un gruppo societario a designare molteplici rappresentanti, ovvero uno per ogni società facente parte del gruppo.

Un limite a tale regola viene, tuttavia, fissato nell'articolo 3(3) della proposta di Direttiva, in considerazione del fatto che il rappresentante legale in questione dovrebbe fungere non solo da destinatario di ordini e decisioni nazionali, ma anche di quelli emessi sulla base degli strumenti di cooperazione giudiziaria penale adottati dall'Unione ai sensi dal capo 4 del Titolo V del Trattato sul Funzionamento dell'Unione europea finalizzati ad acquisire prove in materia penale, come per esempio la direttiva sull'ordine europeo di indagine penale, la Convenzione del 2000 sull'assistenza giudiziaria e l'ordine europeo di produzione di prove elettroniche contemplato dalla nuova proposta di Regolamento: si tratta, dunque, sia di strumenti che permettono la notifica diretta degli ordini al prestatore di servizi in situazioni transfrontaliere, sia di strumenti basati sulla cooperazione tra autorità giudiziarie[17]. Tenendo conto di questo, la proposta di Direttiva ha dovuto prendere in considerazione la "geometria variabile" esistente nel diritto penale a livello UE, determinata dalla mancata partecipazione della Danimarca agli atti legislativi in materia di cooperazione giudiziaria penale adottati dall'Unione sulla base del menzionato Capo 4 del Titolo V del TFUE, nonché dal diritto del Regno Unito e dell'Irlanda di esercitare rispetto ad essi il diritto di aderire o meno (cosiddetto "*opt-in*"): da questo deriva, infatti, che a taluni strumenti di cooperazione giudiziaria penale non partecipano tutti gli Stati membri. Ove, pertanto, un rappresentante legale venisse designato da un *provider* in uno Stato membro a cui non si applica lo strumento di cooperazione giudiziaria penale di interesse, non potrebbe essere destinatario di una decisione o di un ordine emesso in forza di questo. Pertanto, al fine di scongiurare l'indebolimento dell'efficacia della normativa UE in materia, la proposta di Direttiva prevede l'obbligo per il prestatore che offra servizi in Stati membri che partecipano ai rilevanti strumenti UE di cooperazione giudiziaria penale di designare almeno un rappresentante legale in uno di essi: tale obbligo deve essere imposto al *provider* dagli Stati membri che partecipano allo strumento giuridico pertinente.

Sulla base di tali considerazioni possiamo provare a formulare un esempio: in linea generale l'Italia non potrebbe obbligare Facebook a designare un legale rappresentante nel proprio territorio se tale *provider* ne avesse già designato uno in Irlanda, dove ha la propria sede di stabilimento. Tuttavia, l'Italia potrebbe esigere da Facebook la nomina di un legale rappresentante sul proprio territorio per la notifica di provvedimenti di acquisizione della prova basati su un ordine investigativo europeo, atteso che l'Irlanda ha deciso di non aderire alla direttiva 2014/41/EU che prevede tale strumento di cooperazione giudiziaria: ciò sempre che Facebook non abbia già nominato

[17] Vedasi al riguardo il considerando 8 della proposta di Direttiva.

anche un secondo rappresentante legale in uno Stato membro diverso dall'Irlanda, a cui si applichi la direttiva 2014/41/EU in parola.

Appare, inoltre, rilevante segnalare fin d'ora l'opportunità di leggere il menzionato articolo 3(3) della proposta di Direttiva congiuntamente:

– all'articolo 1(3) e al considerando (11) della proposta di Direttiva, nei quali si chiarisce che – nonostante la designazione di un rappresentante legale – uno Stato membro può continuare a rivolgersi ad un prestatore di servizi stabilito sul proprio territorio sia in situazioni puramente nazionali sulla base del proprio diritto interno, sia in virtù della legislazione UE, a seguito alla ricezione di una richiesta di assistenza giudiziaria penale o di mutuo riconoscimento;

– al nuovo comma 1a) dell'articolo 3 e al pertinente considerando (24a) introdotti dall'orientamento generale del 7 dicembre 2018 sulla proposta di Regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche, secondo cui il Regolamento non si applica ai procedimenti nazionali finalizzati a fornire assistenza giudiziaria reciproca (*mutual legal assistence*) in materia penale ad un altro Stato membro o a un paese terzo. Il principio che ha inspirato questa norma sembra essere quello che la richiesta di assistenza vada indirizzata all'autorità competente dello Stato membro in cui è stabilito o rappresentato il prestatore di servizi, affinché possa essere da questa eseguita utilizzando misure di diritto interno atte ad ottenere la prova digitale dal *service provider* (ovvero senza bisogno di emettere un provvedimento transnazionale come l'ordine europeo di produzione della prova elettronica), previa verifica dei requisiti di ammissibilità della richiesta stessa previsti dal pertinente strumento internazionale di reciproca assistenza giudiziaria.

Affinché questo sistema possa funzionare in modo efficiente e tutte le autorità giudiziarie degli Stati membri possano conoscere in maniera certa e costantemente aggiornata dove si trovano e chi sono i rappresentanti legali designati dai prestatori di servizi nel territorio dell'Unione, l'articolo 6 della proposta di Direttiva prevede l'istituzione di un meccanismo di coordinamento basato sulla designazione, da parte di ciascuno Stato membro, di una o più autorità centrali competenti a garantire l'applicazione coerente e proporzionata della Direttiva, anche attraverso lo scambio di tutte le informazioni e l'assistenza reciproca necessaria, soprattutto con riferimento all'attuazione delle misure esecutive. Tali designazioni a livello nazionale vengono comunicate alla Commissione europea, che a sua volta fa circolare una lista tra gli Stati membri contenente l'elenco delle autorità centrali designate, pubblicandola altresì per agevolare i prestatori di sevizi nella trasmissione di notifiche agli Stati membri in cui i loro rappresentanti legali risiedono o sono stabiliti.

L'autorità centrale designata dallo Stato membro costituisce l'interlocutore principale del *service provider* che in tale Stato membro abbia deciso di nominare il proprio rappresentante legale, il quale deve essere ivi residente o stabilito: invero, ai sensi dell'articolo 4 della proposta di Direttiva, il prestatore di servizi è tenuto a notificare all'autorità centrale l'identità e i dati di contatto del proprio rappresentante legale, nonché eventuali aggiornamenti di queste informazioni. All'atto della notifica, il *provider* deve, altresì, indicare la lingua o le lingue in cui le autorità nazionali competenti potranno rivolgersi al proprio rappresentante legale, tra cui deve figurare

necessariamente almeno una delle lingue ufficiali dello Stato membro in cui il rappresentante legale risiede o è stabilito. Ove, poi, il prestatore di servizi designi più rappresentanti legali, può dare indicazioni che consentano alle autorità nazionali competenti di decidere a quali di essi rivolgersi. La norma prevede che tali indicazioni non siano vincolanti per le autorità nazionali, ma che queste possano discostarsene solo adducendo una espressa giustificazione.

Attesa l'importanza di tutte le informazioni in parola, l'articolo 4(4) prevede sia l'obbligo per il prestatore di servizi di renderle pubbliche (ad esempio attraverso il proprio sito web), pena l'imposizione di sanzioni, sia l'obbligo per le autorità centrali degli Stati membri di pubblicarle su un apposito sito del portale europeo della giustizia elettronica, al fine di agevolare il coordinamento tra gli Stati membri e il ricorso al rappresentante legale da parte delle autorità competenti di un altro Stato membro.

La proposta di Direttiva prevede, infine, agli articoli 7 ed 8, un termine molto breve per il recepimento da parte degli Stati membri, indicato in sei mesi dalla sua entrata in vigore, nonché un meccanismo di valutazione da parte della Commissione europea da portarsi a termine entro cinque anni dall'entrata in vigore dello strumento. Ai sensi del considerando (25), tale valutazione dovrà essere basata sui cinque criteri di efficienza, efficacia, pertinenza, coerenza e valore aggiunto generalmente utilizzati dall'UE nel valutare l'opportunità di adottare nuove misure normative e dovrà contenere un'analisi sulla eventuale necessità di ampliarne l'ambito di applicazione.

3. La proposta di Regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (COM(2018)225 final) alla luce dell'orientamento generale del Consiglio UE del 7 dicembre 2018 (ST15292/18).

Per quanto attiene, invece, alla seconda iniziativa legislativa della Commissione europea sopra menzionata, ovvero la proposta di Regolamento sugli ordini europei di produzione e conservazione delle prove elettroniche in materia penale, essa mira a semplificare e rendere più rapido il processo di "messa in sicurezza" e acquisizione di prove digitali detenute da prestatori di servizi stabiliti o rappresentati nella giurisdizione di un altro Stato membro, prevedendo la trasmissione del provvedimento penale di conservazione o acquisizione della *e-evidence* direttamente dall'autorità nazionale richiedente al rappresentante legale designato dal *service provider* sul territorio europeo, con obbligo per quest'ultimo di ottemperare consegnandole direttamente i dati, salva la sussistenza di specifici e tassativi motivi che lo impediscano e *senza poter opporre ragioni legate al luogo di conservazione dei dati*. Tale impianto è stato sostanzialmente mantenuto nel testo dell'orientamento generale del Consiglio UE sulla proposta di Regolamento in parola, adottato dai Ministri della Giustizia degli Stati membri il 7 dicembre 2018 (da qui in avanti, "orientamento generale").

L'obiettivo è, dunque, quello di istituire ordini europei di conservazione e di produzione della prova elettronica che abbiano carattere vincolante per il *service provider* che offre servizi nell'Unione. È bene sottolineare fin da ora che tali strumenti possono essere utilizzati dalle autorità nazionali competenti *solo in situazioni transfrontaliere*, ossia

nei casi in cui il prestatore di servizi sia stabilito o rappresentato in un altro Stato membro. Ove, invece, sia stabilito o rappresentato sul proprio territorio nazionale, le autorità requirenti dovranno continuare ad avvalersi delle misure normative messe a disposizione dal diritto interno. Nel nostro Paese, per esempio, il mezzo investigativo utilizzato dal pubblico ministero per ottenere la prova digitale dal *service provider* che abbia una sede di stabilimento o un rappresentante legale sul territorio italiano, è l'ordine di esibizione ai sensi dell'art. 256 c.p.p. Per quanto attiene, invece, alla conservazione della prova digitale, il sequestro probatorio di dati informatici presso fornitori di servizi previsto dall'art. 254 bis c.p.p. sembra essere lo strumento nazionale che più si avvicina concettualmente all'ordine europeo di conservazione, anche attesa la possibilità per l'autorità inquirente italiana di ordinare al fornitore di servizi la conservazione e adeguata protezione dei dati originali[18].

3.1. Il rapporto con l'ordine europeo di indagine penale.

È bene evidenziare, in via preliminare, che gli ordini europei di produzione e di conservazione di prove elettroniche sono stati concepiti per affiancare e non per sostituire gli strumenti di cooperazione giudiziaria già attualmente esistenti, che potranno dunque continuare ad essere utilizzati dalle autorità nazionali competenti quando li ritengano pertinenti ed appropriati. Si pensi, in particolare, all'ordine europeo di indagine penale, che ha in gran parte sostituito gli strumenti di cooperazione giudiziaria previsti dalla Convenzione del 2000 relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'UE[19] e che può avere ad oggetto qualsiasi atto di

[18] In tema di sequestro di dati informatici, vedasi la sentenza delle Sezioni Unite della Suprema Corte n. 40963/2017, che affronta molte questioni di diritto di grande complessità, tra cui il portato della Convenzione di Budapest sul *cybercrime* (ratificata nel nostro Paese con l. 18 marzo 2008, n. 48, vedasi nota 8) e la sua capacità di incidere trasversalmente sul diritto delle prove penali e sulle attività di indagine ben al di là del circoscritto settore inerente all'accertamento dei reati informatici; la distinzione tra le componenti *hardware* e *software* di un sistema informatico, funzionale alla definizione del concetto di dato o documento informatico quale *res* in sé, altra e distinta dal supporto in cui è incorporata; principi in materia di sequestro, tra cui la netta affermazione del rilievo da attribuirsi al principio di proporzionalità in una materia in cui non sempre se ne è fatto un buon governo; i principi ricavabili dalla CEDU in materia di diritto al rispetto della vita privata e familiare e di libertà di espressione come interpretati dalla Corte di Strasburgo; regole sulla impugnazione in ordine alla esatta conformazione dell'interesse ad impugnare. La sentenza, inoltre, pare incidere sulla nozione stessa di sequestro, ponendosi quale discrimine tra i casi in cui la restituzione della cosa risolve il provvedimento ablativo e i casi nei quali la restituzione in sé, accompagnata dalla clonazione della memoria elettronica, non scioglie il vincolo di indisponibilità, che si perpetua, appunto, con e nella effettuazione della copia. Si rimanda, sul punto, alla nota a sentenza di G. TODARO, *Restituzione di bene sequestrato, estrazione di copia, interesse ad impugnare: revirement delle Sezioni Unite*, in questa *Rivista*, fasc. 11/2017, p. 157 ss.

[19] Vedasi al riguardo M. DANIELE, *L'ordine europeo di indagine penale entra a regime. Prime riflessioni sul d.lgs. n. 108 del 2017*, cit., p. 208. Il sistema rogatoriale continua, tuttavia, ad applicarsi nella cooperazione giudiziaria con Irlanda e Danimarca che hanno esercitato l'*opt-out* rispetto alla Direttiva 2014/41/UE sull'ordine europeo di indagine penale. Si evidenzia, peraltro, che l'Irlanda ha firmato il 29 maggio 2000 la Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri della UE ma non l'ha ancora ratificata.

indagine, ivi compresa l'acquisizione della prova elettronica. Esso, tuttavia, prevede la trasmissione della richiesta dall'autorità giudiziaria di emissione a quella di esecuzione, la quale non ha l'obbligo di eseguirla subito e anzi deve sottoporla ad una serie di controlli che possono condurre a rinviarne o, addirittura, a rifiutarne l'esecuzione.

Pertanto, ove l'acquisizione della prova elettronica sia l'unico atto di indagine transnazionale che l'autorità nazionale competente deve porre in essere, sarà tendenzialmente più rapido ed efficace emanare un ordine di acquisizione della prova elettronica piuttosto che un ordine europeo di indagine penale, atteso che il primo consente la trasmissione diretta della richiesta al *service provider* e non richiede il coinvolgimento dell'autorità giudiziaria del paese di esecuzione, se non nei limiti che vedremo in seguito. Invece, quando l'autorità nazionale deve compiere diversi atti di indagine nello Stato membro di esecuzione (e non solo l'acquisizione di prove elettroniche), potrebbe preferire ricorrere all'ordine europeo di indagine penale, al fine di formulare un'unica richiesta all'autorità giudiziaria dello Stato di esecuzione.

Ne consegue che – al fine di garantire l'effettiva utilità investigativa dei nuovi strumenti e, in ultima analisi, assicurarne il concreto utilizzo nella pratica giudiziaria – è necessario che i meccanismi procedurali dell'ordine di conservazione e di acquisizione della prova elettronica vengano elaborati secondo moduli di massima semplificazione che ne costituiscano il valore aggiunto rispetto ad altri strumenti di cooperazione giudiziaria già esistenti. In altre parole, è evidente che qualora l'ordine di produzione europeo non mantenga, nel corso del negoziato di trilogo a Bruxelles, quelle caratteristiche di maggiore "appetibilità" in termini di rapidità ed efficienza di acquisizione della prova elettronica, le autorità procedenti continueranno a ricorrere agli strumenti di cooperazione già disponibili.

Tale basilare rilievo è da tenersi nella massima considerazione con riferimento ad un aspetto di cui si parlerà in seguito, ovvero il meccanismo di notifica dell'ordine di produzione all'autorità dello Stato di esecuzione, che è stato introdotto dal Consiglio UE nel testo dell'orientamento generale adottato il 7 dicembre 2018 (vedasi articolo 7a) e che dovrebbe accompagnare in parallelo l'inoltro in via diretta degli ordini di produzione dalle autorità emittenti ai *service providers* (cosiddetta *tandem procedure*). Come vedremo, la valenza da attribuire a questo meccanismo di notifica ed i conseguenti poteri di rifiuto dell'ordine di produzione da riconoscersi o meno all'autorità "notificata" dello Stato di esecuzione costituisce un aspetto ancora molto controverso tra gli Stati membri, che continuerà ad essere discusso nel negoziato di trilogo con il Parlamento UE e che rischia di depotenziare in maniera rilevante l'efficacia investigativa del nuovo strumento, rendendolo una sorta di "duplicato" dell'ordine europeo di indagine penale, ove alla fine prevalesse l'orientamento di un coinvolgimento sostanziale (e non meramente informativo) dell'autorità dello Stato di esecuzione già nella fase di trasmissione dell'ordine di produzione.

3.2. Autorità nazionali competenti ad emettere gli ordini europei di produzione e di conservazione della prova elettronica.

L'articolo 4 dell'orientamento generale prevede che gli ordini di produzione riguardanti dati relativi alle operazioni o al contenuto, atteso il loro carattere maggiormente invasivo della libertà personale e potenzialmente lesivo di diritti fondamentali, debbano essere emessi o autorizzati da un giudice o da un organo giurisdizionale o da un giudice addetto alle investigazioni (nel nostro ordinamento, tale figura coinciderebbe con quella del giudice per le indagini preliminari, mentre in quello francese con il *juge d'instruction*), mentre quelli riguardanti i dati relativi agli abbonati o agli accessi possono essere emessi o autorizzati anche da un pubblico ministero. Quanto, invece, agli ordini di conservazione, considerata la loro mera finalità di "congelamento" del dato informatico, possono essere emessi o autorizzati da un'autorità giudicante ma anche da un pubblico ministero.

Un elemento che può essere utile segnalare fin d'ora è che nel nostro ordinamento il pubblico ministero può emettere un ordine di esibizione ai sensi dell'art. 256 c.p.p. indirizzato al prestatore di servizi che abbia una sede di stabilimento o un rappresentante legale sul territorio italiano, senza necessità di autorizzazione da parte del giudice per le indagini preliminari e ciò indipendentemente dal tipo di dati informatici di cui dispone l'acquisizione. Nel caso di utilizzo dell'ordine europeo di produzione dovrà, invece, chiedere l'autorizzazione al G.I.P. nel caso in cui voglia ottenere dal *service provider* stabilito o rappresentato in un altro Stato membro dati relativi alle operazioni o al contenuto.

Nelle ipotesi di autorizzazione dell'ordine di produzione o di conservazione, l'autorità che l'ha effettuata può anche essere considerata - ai sensi dell'articolo 4(4) dell'orientamento generale – l'autorità di emissione ai fini della trasmissione al prestatore di servizi del certificato europeo di produzione o di conservazione della prova elettronica (di cui si parlerà in seguito).

Appare rilevante precisare che, ai sensi del nuovo comma 5 dell'articolo 4 introdotto dall'orientamento generale, in casi di emergenza e con riferimento ai soli ordini di produzione e di conservazione di dati relativi agli abbonati o agli accessi, la convalida dell'autorità giudiziaria o del pubblico ministero può essere richiesta successivamente all'emissione dei provvedimenti in parola e comunque non oltre le quarantotto ore (cosiddetta "*ex-post validation*"), a condizione che l'autorità emittente detenga tale potere di agire senza previa autorizzazione, in circostanze simili, nell'ordinamento nazionale di appartenenza. Ove la convalida non venga disposta, l'autorità emittente deve immediatamente revocare l'ordine in questione e deve procedere, secondo le norme del diritto nazionale, a cancellare ogni dato nel frattempo acquisito oppure ad assicurare che lo stesso non venga utilizzato come prova nel procedimento penale.

Si segnala che la formulazione del nuovo comma 5 dell'articolo 4 dell'orientamento generale, riferendosi ai casi di emergenza in cui è ammessa l'emissione degli ordini senza preventiva autorizzazione, indica che tali casi debbano essere "legittimamente previsti" (*validly established*), creando dubbi di interpretazione

rispetto alla definizione di "casi di emergenza" già contenuta dall'articolo 2(15) dell'orientamento generale, ai sensi della quale essi coincidono con le situazioni in cui sussiste una minaccia imminente per la vita o l'integrità fisica di una persona o per un'infrastruttura critica.

3.3. Definizione di "prova elettronica". Esclusione delle intercettazioni in tempo reale. Il problema dei dati criptati.

Nel richiamare, con riferimento ai prestatori di servizi a cui può essere rivolto un ordine di produzione o conservazione della prova elettronica, quanto già detto nel paragrafo dedicato alla proposta di Direttiva sulla nomina di rappresentanti legali da parte dei prestatori di servizi, si reputa opportuno ora soffermarsi brevemente sulla definizione di "prova elettronica" contenuta nell'articolo 2 dell'orientamento generale, che non è stata modificata dall'orientamento generale del Consiglio UE rispetto all'iniziale proposta della Commissione europea[20].

Le categorie di dati che le autorità competenti possono ottenere o conservare con un ordine europeo di produzione o conservazione della *e-evidence* sono i dati relativi agli abbonati, agli accessi, alle operazioni e al contenuto.

I dati relativi agli abbonati e quelli relativi agli accessi sono spesso il punto di partenza per individuare l'identità dell'utente. In particolare, i dati relativi agli abbonati sono quelli riguardanti l'identità di un abbonato o di un cliente (come il nome e la data di nascita), l'indirizzo postale, i dati di fatturazione e pagamento, in numero di telefono e l'indirizzo e-mail forniti. Sono, altresì, i dati relativi al tipo di servizio e alla sua durata (compresi i dati tecnici e i dati che identificano le misure tecniche correlate o le interfacce usate dall'abbonato o dal cliente o a questo fornite e di dati connessi alla convalida dell'uso del servizio), con esclusione delle password o di altri mezzi di autenticazione forniti dall'utente o creati a sua richiesta.

I dati relativi agli accessi sono, invece, quelli generalmente memorizzati nell'ambito di una registrazione di eventi (in altre parole, un "*log server*") per indicare l'inizio e la fine di una sessione di accesso di un utente a un servizio (per esempio, la data e l'ora d'uso; la connessione al servizio e la fine di utilizzo dello stesso, ovvero il *log-in* e il *log-off*). Il più delle volte si tratta di un indirizzo IP o di altro identificatore che individua l'interfaccia di rete usata durante la sessione di accesso. Se l'utente è ignoto, spesso occorre ottenere tali dati prima di poter chiedere al prestatore di servizi i dati relativi agli abbonati che sono correlati a quell'identificatore. È bene precisare che i dati relativi agli accessi non rivelano alcuna informazione sugli interlocutori degli utenti,

[20] Sul concetto di "*digital evidence*" e sul raffronto tra "*digital forensics*" negli Stati Uniti ed in Italia, vedasi G. VACIAGO, *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Torino, 2012, p. 1 ss.; sulla prova digitale e la sua acquisizione e conservazione, L. CUOMO, *La prova digitale*, in *Prova scientifica e processo penale*, a cura di G. Canzio e L. Luparia, Padova, 2018, Parte III, Capitolo 16, p. 669 ss.

laddove invece i dati relativi alle operazioni sono generalmente richiesti per ottenere elementi conoscitivi sui contatti dell'utente e sul luogo in cui questo si trova.

I dati relativi alle operazioni, infatti, sono quelli riguardanti la fornitura del servizio che servono per acquisire informazioni di contesto o supplementari sul servizio stesso e che sono generati o trattati da un sistema informatico del prestatore di servizi, come la fonte e il destinatario di un messaggio o di altro tipo di interazione, i dati sull'ubicazione del dispositivo, la data, l'ora, la durata, le dimensioni, il percorso, il formato, il protocollo usato e il tipo di compressione, a meno che tali dati costituiscano dati relativi agli accessi. Rientrano in questa categoria i metadati delle comunicazioni elettroniche.

Infine, i dati relativi al contenuto sono tutti quelli conservati in formato digitale, come testo, voce, video, immagine o suono, diversi dai dati relativi agli abbonati, agli accessi e alle operazioni.

Tutte le categorie sopra menzionate contengono dati personali e rientrano pertanto nell'ambito di applicazione delle garanzie previste dall'*acquis* europeo sul trattamento e la protezione dei dati di questa tipologia, ma l'intensità dell'impatto della loro acquisizione sui diritti fondamentali cambia evidentemente in maniera sostanziale a seconda del tipo di dato richiesto, tanto che la proposta di Regolamento prevede condizioni diverse per l'ottenimento dei dati relativi agli abbonati e agli accessi da un lato, e dei dati relativi alle operazioni e al contenuto dall'altro, sulle quali torneremo in seguito.

Un aspetto fondamentale da evidenziare è che tutti i dati che rientrano nella definizione di "prova elettronica" devono essere "*conservati* in formato elettronico dal prestatore di servizi o per suo conto *al momento della ricezione* del certificato di ordine europeo di produzione o di conservazione", ai sensi dell'articolo 2(6) dell'orientamento generale. Ciò significa che non può essere disposta dall'autorità nazionale la produzione o la conservazione di dati che vengano registrati dal *service provider* in un tempo futuro rispetto al momento di ricezione del relativo ordine, atteso che tale misura si tradurrebbe di fatto in un'intercettazione e che tale mezzo di ricerca della prova è stato, invece, volontariamente escluso dall'ambito di applicazione della proposta di Regolamento (vedasi il considerando 19 dell'orientamento generale). Si segnala, peraltro, che nel corso del negoziato intercorso in sede COPEN presso il Consiglio UE, taluni Stati membri, tra cui l'Italia, avevano proposto di allargare l'ambito di applicazione del Regolamento sia alle intercettazioni delle comunicazioni *on-line* ("*real-time interception*") che al cosiddetto "accesso diretto" da remoto dell'autorità giudiziaria ai dati disponibili nel *server* del *provider* senza bisogno del coinvolgimento di quest'ultimo ("*direct access to e-evidence*") a seguito della perquisizione e sequestro del dispositivo oppure attraverso l'uso delle credenziali di accesso dell'utente legittimamente acquisite. Questa proposta è stata portata dalla Presidenza bulgara all'attenzione dei Ministri della giustizia nella riunione del Consiglio UE – Giustizia e Affari interni del 4-5 giugno 2018 per riceverne linee politiche di indirizzo[21], ma molte delegazioni hanno espresso perplessità al riguardo e la

[21] Vedasi il documento di discussione del 25 maggio 2018 sottoposto dalla Presidenza bulgara all'attenzione

Commissione europea ha manifestato forte contrarietà, ritenendo che ne sarebbe risultato stravolto l'impianto originario dell'iniziativa normativa, allungando notevolmente i tempi del negoziato e conseguentemente ritardando l'adozione dello strumento, che dovrebbe invece essere adottato in via d'urgenza, auspicabilmente prima delle elezioni parlamentari di maggio 2019, attese le crescenti minacce poste dal terrorismo internazionale. L'opzione in parola è stata, pertanto, abbandonata sotto Presidenza austriaca.

Un'altra disposizione dell'orientamento generale che meriterebbe attenzione nel corso del prossimo negoziato è quella contenuta nel considerando 19, secondo cui i dati devono essere forniti dal prestatore di servizi *a prescindere dal fatto che siano criptati o meno*. Se i dati non sono criptati, *nulla quaestio*. Ove, invece, i dati siano criptati – come succede nella gran parte dei casi - possono verificarsi situazioni diverse a seconda del tipo di criptazione[22].

Prima ipotesi: taluni *service providers*, come Facebook Messenger, hanno un *server* che decritta il messaggio criptato pervenuto dall'utente prima di inoltrarlo – nuovamente criptato – al destinatario finale. Ciò significa che questi prestatori di servizi detengono le chiavi di decrittazione, la cui consegna dovrebbe pertanto essere resa esplicitamente obbligatoria dal Regolamento per il rappresentante del *service provider* nel territorio dell'Unione, congiuntamente a quella dei dati criptati. Questo consentirebbe, peraltro, di superare eventuali eccezioni di giurisdizione legate al fatto che la chiave di decrittazione potrebbe essere detenuta da una società commerciale facente capo al *service*

---

dei Ministri della Giustizia nella riunione del Consiglio UE – Giustizia e Affari interni del 4-5- giugno 2018 (9117/18, Limite, reperibile al seguente *link*): *"4. While welcoming the proposals, a number of delegations regretted the limited scope of the proposed Regulation as it does not address direct access to e-evidence (direct access to data without the assistance of a third party (service provider) as an intermediary), or real-time interception of data. Many delegations felt that these two elements needed to be addressed as they respond to an operational need and thus need to be studied further and in much greater detail. However, opinions are divided as to whether this should be done with a view to including them in the current proposals or rather in parallel to the current proposals so as not to delay or prolong the current negotiations.*

5. As regards real-time interception of data, the following considerations have been made so far:

– this is a sensitive and intrusive measure

– this possibility is provided for in most national laws for domestic circumstances, in the Directive on the European Investigation Order and in the US CLOUD Act; any EU basis for real-time interception of data should be considered in this broader framework and take account of the need to equip Member States' authorities with the full range of tools to fight crime in the digital era [that are at the disposal of their US colleagues]. Moreover, Member States raised that the possibility to cover real-time interception in an Executive Agreement under the US CLOUD Act, on a reciprocal basis, should also be considered as part of the reflection on this measure.

6. As regards direct access to e-evidence, the following considerations have been made so far:

– it is a powerful tool in case of loss of location or non-cooperative service providers, empowering Member States' authorities to remotely access the data available following the search and seizure of a device or the use of lawfully obtained credentials for access to an account;

– there is a wide variation in national laws currently regulating such direct access in the Member States, in particular the safeguards and powers they provide;

– the possible creation of a common EU framework would be beneficial, but such an EU approach should be carefully considered in the light of those divergent national legal frameworks and a number of legal questions, including the appropriate legal basis, should be carefully examined."

[22] Sulla crittografia e la sua disciplina giuridica si rimanda a G. ZICCARDI, *Crittografia e diritto*, Torino, 2003.

provider diversa da quella che lo rappresenta nel territorio dell'Unione e stabilita in un paese terzo. Si ricorda, in proposito, il caso che è stato oggetto in Italia della pronuncia della Suprema Corte a Sezioni Unite n. 46968 del 12 ottobre 2017, ovvero quello delle intercettazioni delle *chat* "*pin to pin*" tra utenti BlackBerry, che avvenivano secondo uno schema operativo analogo: il messaggio veniva inviato criptato dallo *smartphone* del mittente al *server* della società canadese Blackberry, che lo inoltrava al *device* del destinatario, dal quale veniva decrittato e messo in chiaro. Da un punto di vista investigativo, le procedure dirette ad acquisire le conversazioni, nel caso di specie, erano consistite nei seguenti passaggi: la Procura della Repubblica aveva inoltrato alla società italiana rappresentante di Blackberry in Italia, la richiesta dei testi decrittati dei messaggi; la società italiana aveva poi trasmesso la relativa richiesta alla casa madre canadese Blackberry che custodiva le chiavi di decrittazione dei dati identificativi associati ai codici "*pin*", la quale aveva risposto trasmettendo i dati telematici delle captazioni alla propria filiale italiana, che l'aveva infine immessi in originale nel *server* della Procura della Repubblica richiedente. Nel caso di specie, la collaborazione spontanea della casa madre Blackberry stabilita in Canada aveva reso possibile la decrittazione, ma sarebbe stato difficile per l'autorità inquirente italiana costringere Blackberry in Canada a fornire la chiave di decrittazione. Proprio per evitare tali difficoltà, potrebbe essere opportuno precisare nel Regolamento che il rappresentante legale del *service provider* nel territorio dell'Unione è tenuto a fornire anche le chiavi di decrittazione ove possedute dal prestatore di servizi ovunque nel mondo. Tale inciso dovrebbe, peraltro, essere auspicabilmente inserito nell'articolato dello strumento e non solo nei "considerando" iniziali che notoriamente non hanno forza normativa.

Seconda ipotesi: il prestatore di servizi utilizza il sistema di criptazione "*end-to-end*", come per esempio WhatsApp, Telegram e Signal. In tale caso, la crittografia e la decrittazione dei messaggi avviene interamente attraverso gli *smartphone* e cioè il messaggio viene protetto da un lucchetto crittografico collocato dal dispositivo del mittente prima di essere trasmesso, e solo il dispositivo del destinatario del messaggio ne ha le chiavi di decrittazione: non esiste, pertanto, uno "stop" intermedio del flusso di trasmissione che avvenga presso il *server* del prestatore di servizi; inoltre, le chiavi cambiano ad ogni singolo messaggio inviato. Da ciò deriverebbe – secondo quanto sostenuto da questi *providers* – la loro impossibilità di accedere al contenuto dei messaggi o delle conversazioni, non avendone le chiavi di decrittazione. È bene essere consapevoli che in questi casi l'acquisizione di dati criptati attraverso un ordine europeo di produzione della prova elettronica sarebbe totalmente inutile per l'autorità giudiziaria richiedente, considerato che in assenza della chiave di decrittazione risulterebbero illeggibili. Considerato che WhatsApp costituisce uno dei sistemi di comunicazione più utilizzati al mondo, ove l'Unione europea non trovi il modo di obbligare tutti i prestatori di servizi a consegnare i dati in chiaro per finalità di giustizia, indipendentemente dal sistema di criptazione utilizzato, i progressi investigativi nell'acquisizione transnazionale della prova elettronica non potranno che essere esigui e la sensazione potrebbe essere alla fine che la montagna avrà partorito un topolino.

3.4. I procedimenti nazionali in cui possono essere emessi gli ordini europei di produzione e di conservazione della prova elettronica. Il principio di specialità.

Gli ordini europei di produzione e di conservazione della prova elettronica sono atti di indagine che possono essere emessi dalle autorità nazionali competenti solo nell'ambito di procedimenti penali nei confronti di autori, noti o ancora ignoti, di un reato che è già stato commesso, previa valutazione della proporzionalità e della necessità della misura nel caso specifico. I procedimenti in parola possono anche riguardare il reato commesso da una persona giuridica.

Nell'orientamento generale, il Consiglio UE ha integrato il testo dell'articolo 3 originariamente proposto dalla Commissione europea, prevedendo che essi possano essere emessi anche in caso di esecuzione di una condanna a pena detentiva ("*execution of a custodial sentence*", che nel nostro ordinamento corrisponderebbe all'ordine di esecuzione della sentenza penale di condanna previsto dall'art. 656 c.p.p.) o di una misura di sicurezza detentiva definitiva ("*detention order*") quando il soggetto si sia sottratto alla giustizia, purché non siano stati pronunciati in contumacia. La norma sembra ispirarsi alla medesima *ratio* dell'articolo 295, commi 3 e 3 *bis*, del nostro codice di procedura penale, che prevede la possibilità per l'autorità giudiziaria di disporre le intercettazioni nel caso del latitante che si sottragga all'ordinanza di custodia cautelare e – per consolidata interpretazione giurisprudenziale "estensiva" – anche all'ordine di carcerazione[23].

Non può non rilevarsi che sarebbe auspicabile che venissero ricomprese nell'ambito di applicazione dell'articolo 3 in parola anche le ordinanze di custodia cautelare, atteso il pericolo di reiterazione del reato che spesso è alla base di tali misure e del fatto che meccanismi di mutuo riconoscimento tra gli Stati membri dei provvedimenti cautelari custodiali sono già previsti da tempo nella normativa sul mandato di arresto europeo.

Un'ulteriore modifica dell'art. 3 apportata dal Consiglio UE nell'orientamento generale consiste nell'esclusione dall'ambito di applicazione del Regolamento dei procedimenti nazionali che siano stati originati da una richiesta di assistenza giudiziaria reciproca proveniente da un altro Sato membro o da un paese terzo. Si rimanda sul punto a quanto già detto sopra, nel paragrafo dedicato alla proposta di Direttiva sulla nomina di rappresentanti legali da parte dei prestatori di servizi.

Si segnala, inoltre, che è stato introdotto dall'orientamento generale del Consiglio UE un nuovo articolo 12b, nel quale si precisa che la prova elettronica ottenuta attraverso un ordine di produzione può essere utilizzata solo nell'ambito del procedimento nazionale per il quale è stata richiesta ("principio di specialità"), salvo che si tratti di procedimenti nei quali un ordine di produzione avrebbe potuto essere emesso, oppure occorra prevenire una immediata e grave minaccia alla sicurezza pubblica dello Stato di emissione o ai suoi interessi fondamentali. In questi casi lo Stato richiedente può, altresì, trasferire la prova elettronica acquisita ad un altro Stato membro.

---

[23] Vedasi in proposito Cass. n. 48972 del 15 luglio 2009; Cass. n. 15322 del 5 dicembre 2007.

3.5. I presupposti per l'emissione dell'ordine europeo di produzione della prova elettronica e il meccanismo di notifica allo Stato di esecuzione.

L'ordine europeo di produzione della prova elettronica può essere emesso solo se una misura dello stesso tipo è prevista per lo stesso reato in una situazione nazionale comparabile nello Stato di emissione e solo se è necessario e proporzionato (articolo 5 dell'orientamento generale). A tal fine, l'autorità di emissione è chiamata ad assicurare che l'ordine sia effettivamente limitato all'acquisizione dei dati pertinenti e necessari a fini probatori nello specifico procedimento per cui vengono chiesti, tenendo altresì in considerazione l'impatto della misura sui diritti fondamentali (vedasi considerando 29 dell'orientamento generale).

Attesa la potenziale elevata invasività degli strumenti in questione, gli ordini per la produzione di dati relativi agli abbonati o agli accessi possono essere emessi nell'ambito di un procedimento penale per qualsiasi reato, nonché per l'esecuzione di una pena detentiva o di un ordine di detenzione di almeno 4 mesi. Quelli, invece, per la produzione di dati relativi alle operazioni o al contenuto, avendo un maggiore impatto sulle libertà fondamentali, sono soggetti a requisiti più severi e possono essere emessi solo per reati punibili nello Stato di emissione con una pena detentiva della durata massima di almeno 3 anni: non sono, tuttavia, soggetti a tale soglia specifici reati di cui dall'articolo 5(b) dell'orientamento generale ove commessi a mezzo di sistemi informatici, nonché i reati di terrorismo previsti dalla direttiva (UE) 2017/541. Il Consiglio UE ha, inoltre, previsto nell'orientamento generale che gli ordini di produzione di dati relativi alle operazioni o al contenuto possano essere emessi anche per l'esecuzione di una pena detentiva o di un ordine di detenzione di almeno 4 mesi, solo nel caso in cui siano stati disposti dall'autorità giudiziaria per un reato per il quale sarebbe consentita dall'articolo 5 l'emissione di un ordine di produzione di dati relativi alle operazioni o al contenuto.

Un'attenzione particolare è stata, inoltre, dedicata dal Consiglio UE all'ipotesi in cui l'ordine di produzione di dati relativi alle operazioni e ai contenuti venga emesso nei confronti di un soggetto che l'autorità di emissione abbia ragione di ritenere *residente al di fuori del proprio territorio*. Per tale caso, l'orientamento generale del Consiglio UE – modificando in maniera incisiva la proposta iniziale della Commissione – ha previsto norme diverse a seconda che si tratti di un ordine di produzione di dati relativi alle operazioni, che è stato regolato nell'articolo 5(7) e 5(8), ovvero di un ordine di produzione di dati relativi al contenuto, a cui è stato dedicato il nuovo articolo 7a.

In particolare, con riferimento all'ordine di produzione di dati relativi alle operazioni è stato previsto che – ove l'autorità di emissione abbia ragione di ritenere che il soggetto risieda al di fuori del proprio territorio e possa godere nello Stato di esecuzione di immunità o privilegi oppure di limitazioni della responsabilità penale in ragione della tutela della libertà di stampa o di espressione (come, ad esempio, nel caso degli avvocati, dei ministri di culto o dei giornalisti) - l'autorità di emissione debba chiedere chiarimenti alle autorità competenti dello Stato di esecuzione prima di emettere

l'ordine di produzione e debba eventualmente revocarlo od adattarlo tenendo conto dei limiti rappresentati dallo Stato di esecuzione *come se fossero previsi dal proprio ordinamento*. Questa norma appare importante soprattutto perché esplicita un obbligo di rispetto del diritto interno dello Stato di esecuzione da parte dell'autorità di emissione e si applica anche al caso in cui la divulgazione dei dati sulle operazioni potrebbe incidere su un interesse fondamentale dello Stato di esecuzione, come la sicurezza e la difesa nazionali.

Riguardo, invece, all'ordine di produzione di dati relativi al contenuto, riferibili ad un soggetto per il quale l'autorità di emissione abbia ragione di ritenere che risieda al di fuori del proprio territorio, il nuovo articolo 7a dell'orientamento generale ha introdotto un meccanismo di notifica che è stato molto controverso nel corso del negoziato a Bruxelles. In particolare, tale meccanismo prevede che l'autorità di emissione notifichi contemporaneamente l'ordine di produzione in parola al rappresentante legale del prestatore di servizi ed all'autorità competente dello Stato di esecuzione. Quest'ultima può informare l'autorità di emissione prima possibile (e comunque non oltre dieci giorni dalla notifica) della sussistenza di eventuali circostanze previste dall'articolo 5(7) di cui abbiamo già parlato (ovvero dell'esistenza nel proprio ordinamento di immunità, privilegi, limitazioni della responsabilità penale in relazione alla tutela della libertà di stampa o di espressione, motivi di potenziale lesione degli interessi fondamentali dello Stato di esecuzione). In tale caso, l'autorità di emissione dovrà valutare queste circostanze come se fossero previste dalla propria legge nazionale e dovrà eventualmente revocare o adattare l'ordine già emesso, informandone il *service provider*.

È rilevante sottolineare che questo meccanismo di notifica all'autorità competente dello Stato di esecuzione avviene in parallelo alla notifica dell'ordine di produzione al prestatore di servizi *e non sospende in alcun modo* l'obbligo di quest'ultimo di adempiere all'ordine: per questa ragione la procedura è stata battezzata nel corso del negoziato "*tandem procedure*".

Può essere interessante sapere che la formulazione del nuovo articolo 7a dell'orientamento generale appena descritta è stato il risultato di un compromesso in sede di negoziato tra gli Stati membri di non facile raggiungimento. Invero, fin dalle prime riunioni di lavoro del gruppo COPEN è apparso evidente che l'aver previsto la possibilità di indirizzare l'ordine di produzione o conservazione della prova elettronica direttamente al *service provider*, se da un lato costituisce la novità più significativa in termini di potenziale accelerazione e fluidificazione delle procedure investigative nazionali, costituisce dall'altro anche il profilo di maggiore delicatezza in termini di cessione della sovranità statale, poiché viene escluso – se non nei limitati casi che vedremo in seguito – l'intervento dello Stato di esecuzione: tutto, dunque, si basa sul principio del mutuo riconoscimento delle decisioni giudiziarie che – nell'impianto normativo originario della proposta della Commissione – trova un suo bilanciamento nelle ampie garanzie di controllo giurisdizionale previste dal Regolamento, nonché nei poteri attribuiti al *provider* di opposizione all'esecuzione degli ordini di produzione e conservazione, a seguito della quale si attiva la competenza dell'autorità giudiziaria dello Stato di esecuzione (se ne parlerà in seguito).

Alla fine del negoziato in sede di Consiglio UE, nella riunione del 7 dicembre 2018 in cui i Ministri della Giustizia hanno approvato l'orientamento generale, Finlandia, Germania, Grecia, Lettonia, Repubblica ceca e Ungheria hanno mantenuto una riserva sul testo di questa norma, ritenendo che dovrebbe essere modificata nel corso del negoziato di trilogo con il Parlamento europeo per estenderne l'applicabilità agli ordini di produzione dei dati sulle operazioni (e non solo di contenuto) e per inserire una previsione finalizzata a consentire all'autorità notificata dello Stato di esecuzione di esercitare un potere di rifiuto dell'ordine di produzione in caso di rintracciata violazione dei diritti fondamentali. Su posizione diametralmente opposta si sono attestati Belgio, Bulgaria, Estonia, Francia, Irlanda, Italia, Polonia, Portogallo e Spagna, che hanno espresso una riserva sull'introduzione del meccanismo di notificazione ora previsto dagli articoli 5(7) e 7a, ritenendo preferibile l'impianto originario della proposta della Commissione europea, che prevede la notifica diretta al *service provider* senza alcun coinvolgimento dell'autorità competente dello Stato di esecuzione se non nel caso di inadempimento o di opposizione del prestatore di servizi: la maggioranza degli Stati membri ha, pertanto, ritenuto che il valore aggiunto di questa iniziativa legislativa sia da rintracciarsi proprio nella richiesta di acquisizione trasmessa *direttamente* dall'autorità giudiziaria al *provider*, a cui non si deve rinunciare, pena l'adozione di una sorta di duplicato dell'ordine europeo di indagine penale privo di qualunque "attrattività" per le autorità investigative.

La posizione di compromesso raggiunta tra gli Stati membri sul meccanismo di notificazione sopra descritto è stata specularmente recepita nel nuovo articolo 12a dell'orientamento generale con riferimento all'*utilizzo nel procedimento penale* dei dati acquisiti da parte dell'autorità di emissione. In particolare, si prevede che – ove l'autorità di emissione abbia già ottenuto i dati richiesti con un ordine di produzione e tali dati appartengano ad un soggetto non residente nel territorio dello Stato di emissione rispetto al quale l'autorità emittente venga informata che sussistono forme di protezione nell'ordinamento dello Stato di esecuzione relative ad immunità o privilegi o limitazioni della responsabilità penale in ragione della tutela della libertà di stampa o di espressione – le autorità competenti dello Stato di emissione devono assicurare che tali circostanze vengano prese in considerazione nell'ambito del procedimento penale come se fossero previste dalla propria normativa interna.

Rimane ferma, in tutti i casi sopra menzionati, la possibilità per la competente autorità dello Stato di emissione di chiedere la revoca dell'immunità o del privilegio all'autorità che abbia il potere di farlo, sia essa dello Stato di esecuzione o di un altro Stato membro o di un paese terzo o all'organizzazione internazionale interessata.

3.6. I presupposti per l'emissione dell'ordine europeo di conservazione della prova elettronica.

L'ordine europeo di conservazione della prova elettronica, analogamente all'ordine europeo di produzione, può essere trasmesso dall'autorità competente dello Stato membro direttamente al rappresentante legale del prestatore di servizi che si trovi al di fuori della propria giurisdizione, affinché questo provveda alla preservazione dei

dati digitali, evitandone la rimozione, la cancellazione o la modifica, in vista di una successiva richiesta di produzione dei medesimi, che potrà avvenire attraverso strumenti di assistenza giudiziaria reciproca, un ordine europeo di indagine penale oppure un ordine europeo di produzione della prova elettronica. Lo scopo è, dunque, quello di "congelare" i dati pertinenti in situazioni in cui potrebbe occorrere più tempo per chiederne od ottenerne la produzione, ad esempio quando vengano utilizzati i canali della cooperazione giudiziaria.

L'ordine di conservazione può essere emesso nel procedimento penale relativo a qualsiasi reato oppure per l'esecuzione di una sentenza di condanna a pena detentiva o di un ordine di detenzione di almeno 4 mesi, previa valutazione della necessità e della proporzionalità nel singolo caso. Non è stata prevista alcuna soglia di pena relativamente al reato per il quale può essere richiesto, sulla base della considerazione che l'ordine europeo di indagine penale può essere emesso per qualsiasi reato senza limiti di soglia e pertanto anche l'ordine europeo di conservazione deve trovare sotto questo aspetto la medesima disciplina, atteso il suo carattere "servente".

Come già sopra evidenziato, per consentire alle autorità inquirenti di agire rapidamente e considerato che la richiesta di produrre i dai sarà adottata successivamente, dopo che tutte le condizioni saranno nuovamente esaminate, l'ordine europeo di conservazione può essere emesso, autorizzato o convalidato anche da un pubblico ministero.

3.7. Il destinatario degli ordini europei relativi alla prova elettronica e i certificati di ordine europeo di produzione (EPOC) e di ordine europeo di conservazione (EPOC-PR).

L'ordine europeo di produzione e quello di conservazione della prova elettronica devono essere trasmessi dall'autorità competente dello Stato di emissione al rappresentante legale designato dal *service provider* sul territorio dell'Unione ai sensi della proposta di Direttiva sulla nomina dei rappresentanti legali da parte dei prestatori di servizi di cui abbiamo già parlato.

Ove il *service provider* non abbia designato alcun rappresentante legale, gli ordini possono essere rivolti a qualsiasi stabilimento del prestatore di servizi nell'Unione. Questa ipotesi di riserva è finalizzata a garantire la tenuta del sistema qualora il prestatore di servizi non abbia (ancora) nominato il proprio rappresentante perché la Direttiva non è stata ancora recepita dagli Stati membri e dunque non ha l'obbligo giuridico di farlo, oppure perché tale obbligo non gli si applica in quanto è stabilito od opera solo in uno Stato membro.

La trasmissione degli ordini deve essere effettuata sotto forma di un certificato di ordine europeo di produzione (EPOC, *European Production Order Certificate*) o di un certificato di ordine europeo di conservazione (EPOC-PR, *European Preservation Order Certificate*), che il rappresentante legale del *provider* è tenuto a ricevere e ad eseguire tempestivamente. Ove tuttavia non adempia, l'articolo 7 dell'orientamento generale prevede due situazioni in cui l'autorità di emissione può indirizzare gli ordini a qualsiasi stabilimento del prestatore di servizi nell'Unione: in caso di emergenza, quando

l'autorità di emissione abbia chiesto di riscontrare un ordine di produzione entro sei ore ai sensi dell'articolo 9(2) e il rappresentante legale non l'abbia fatto; quando l'autorità di emissione ritenga che l'inadempimento del rappresentante legale ad ottemperare ad un ordine di produzione o di conservazione stia cagionando un chiaro rischio di perdita dei dati.

Per quanto attiene al formato dei certificati di ordine europeo di produzione (EPOC) e di ordine europeo di conservazione (EPOC-PR), vale innanzitutto precisare che i modelli di entrambi sono contenuti negli allegati I e II della proposta di Regolamento e devono essere tradotti dall'autorità di emissione in una delle lingue ufficiali dell'Unione indicata dal prestatore di servizi, anche all'atto di designazione del proprio rappresentante legale, come abbiamo visto analizzando la proposta di Direttiva sulla nomina dei rappresentanti legali da parte dei prestatori di servizi; ove tale scelga dell'idioma non sia stata compiuta dal *provider*, l'articolo 8(5) dell'orientamento generale prevede che la traduzione debba avvenire in una delle lingue ufficiali dello Stato membro in cui si trova il rappresentante legale del prestatore di servizi.

Lo scopo dei certificati è di fornire tutte le informazioni necessarie al destinatario in un formato standardizzato, escludendo dati sensibili contenuti negli ordini di produzione e di conservazione come quelli relativi alla necessità o alla proporzionalità di tali provvedimenti investigativi, per evitare di compromettere la segretezza e il buon esito delle indagini.

Riguardo alle modalità di trasmissione dei certificati in parola dall'autorità di emissione al rappresentante legale del prestatore di servizi, l'articolo 8(2) dell'orientamento generale prevede che debba trattarsi di canali sicuri che consentano al destinatario la verifica dell'autenticità dell'atto e la certificazione del flusso delle comunicazioni. Viene precisato, inoltre, che possono essere piattaforme appositamente messe a disposizione dai *providers* oppure istituite dagli Stati membri o dall'Unione europea come per esempio eCodex e SIRIUS.

Ove i certificati siano incompleti, inesatti o non contengano elementi sufficienti affinché il prestatore di servizi possa ottemperarvi, il destinatario deve contattare l'autorità di emissione per chiedere chiarimenti attraverso un modulo anch'esso standardizzato e contenuto nell'allegato III della proposta di Regolamento (articoli 9(3) e 10(4) dell'orientamento generale). Questo modulo costituisce, più in generale, lo strumento formale attraverso cui deve svolgersi il dialogo tra il destinatario e l'autorità di emissione per qualsiasi questione inerente all'esecuzione dei certificati, come per esempio in caso di impossibilità per il rappresentante legale del prestatore di servizi di fornire o conservare i dati per causa di forza maggiore o per impossibilità materiale (ad esempio quando la persona i cui dati vengono richiesti non è cliente del provider o quando i dati sono stati legittimamente cancellati prima della ricezione dell'ordine). L'autorità di emissione deve essere immediatamente messa a conoscenza di tali circostanze per reagire velocemente e rivalutare la propria strategia investigativa.

Per quanto attiene ai tempi previsti per l'adempimento da parte del rappresentante legale del *provider*, in caso di ordine di acquisizione della prova elettronica l'articolo 9(1) e (2) dell'orientamento generale prevede che il destinatario debba trasmettere i dati all'autorità di emissione (o ad altra autorità investigativa

eventualmente indicata nell'EPOC) entro dieci giorni dalla ricezione del certificato, anche se quest'ultima può stabilire un termine più breve ove giustificato o addirittura chiedere una risposta entro sei ore in casi di emergenza. Nel caso, invece, dell'ordine di conservazione della prova elettronica, l'articolo 10 (1) e (2) prevede che il destinatario ha l'obbligo di conservare i dati per sessanta giorni, a meno che l'autorità di emissione non comunichi al rappresentante legale del *service provider* che il procedimento per la relativa richiesta di acquisizione è stato avviato (per esempio, mandando in traduzione una richiesta di assistenza giudiziaria), nel qual caso quest'ultimo è tenuto a preservare i dati per tutto il tempo necessario a riscontrare la richiesta di produzione. Ove l'autorità di emissione decide di non procedere più in tal senso, deve darne immediata notizia al rappresentante legale del *provider*, poiché i dati dovrebbero essere congelati solo per il tempo necessario a consentire la presentazione della successiva richiesta di produzione.

Un aspetto, infine, sul quale l'attenzione si è particolarmente soffermata in sede di negoziato in gruppo COPEN è stato quello del bilanciamento tra la necessità investigativa di mantenere riservata la richiesta di acquisizione o di conservazione della prova elettronica da un lato, e l'esigenza di assicurare alla persona i cui dati vengono richiesti o conservati di venire a conoscenza della misura disposta dall'autorità giudiziaria e conseguentemente poter esercitare i diritti a propria tutela. Il risultato di questi lavori è stato il nuovo testo dell'articolo 11 dell'orientamento generale, che prevede un generale divieto da parte del *service provider* di informare la persona i cui dati siano stati richiesti o preservati, a meno che non sia la stessa autorità di emissione a chiedere esplicitamente al prestatore di servizi di informare il soggetto interessato: in tal caso essa dovrà fornire anche indicazioni dei rimedi che possono essere da questo esperiti contro la misura adottata. Nel caso in cui l'autorità di emissione non chieda al *provider* di informare la persona interessata, deve provvedervi l'autorità di emissione stessa, che potrà ritardare questo adempimento solo nella misura in cui ciò risponda a criteri di necessità e proporzionalità nell'ambito del procedimento penale che ha originato l'ordine di acquisizione o conservazione della prova elettronica. L'unico limite previsto a tale obbligo è per il caso di ordini che attengano ai dati relativi agli abbonati o agli accessi, quando l'autorità di emissione ritenga che l'informazione della persona interessata possa ledere i diritti fondamentali o gli interessi legittimi di un terzo, da reputarsi prevalenti rispetto alla tutela del soggetto a cui i dati appartengono.

3.8. La procedura di riesame in caso di conflitto dell'ordine di produzione con la legislazione di un paese terzo. Il mandato alla Commissione europea a negoziare un accordo con gli Stati Uniti.

Un possibile ostacolo al funzionamento dell'ordine di produzione è stato individuato dalla Commissione europea nel fatto che il *service provider* possa rifiutare la consegna dei dati, adducendo che ad essa ostano norme di divieto di uno Stato terzo al cui rispetto sia tenuto. Al fine di superare questo aspetto critico, nella proposta di Regolamento era stata prevista una procedura aggravata in base alla quale, di fronte ad una simile eccezione, l'autorità emittente avrebbe dovuto demandare la questione ad una diversa autorità giurisdizionale nazionale, per un "riesame" dell'ordine di

produzione alla luce dell'obbligo confliggente invocato dal *service provider*. La procedura era concepita in modo differenziato a seconda che il divieto di consegna dei dati fosse volto alla tutela di diritti fondamentali dell'individuo o di interessi fondamentali del paese terzo (articolo 15), ovvero tutelasse interessi di natura diversa (articolo 16).

In particolare, l'impianto originario della proposta normativa prevedeva, all'articolo 15, che il rappresentante legale del *service provider* potesse attivare tale procedura innanzi alla competente autorità giurisdizionale dello Stato di emissione, qualora l'ottemperanza all'ordine di produzione determinasse la violazione della legislazione di un paese terzo finalizzata alla tutela dei diritti fondamentali delle persone interessate o degli interessi fondamentali del paese terzo connessi alla sicurezza o alla difesa nazionali. La valutazione di merito sulla normativa dello Stato terzo era destinata a spingersi sino a verificare "se il diritto del paese terzo, anziché tutelare i diritti fondamentali o interessi fondamentali del paese terzo connessi alla sicurezza o alla difesa nazionali, intenda manifestamente tutelare altri interessi o proteggere attività illecite dalle richieste delle autorità di contrasto nell'ambito delle indagini penali" (così recita l'articolo 15.4 della proposta della Commissione). Inoltre, qualora all'esito del riesame l'autorità giurisdizionale dello Stato di emissione avesse ritenuto di voler insistere nella richiesta dei dati, la procedura prevedeva una consultazione obbligatoria con lo Stato terzo, il cui eventuale parere negativo avrebbe dispiegato un effetto ostativo vincolante per lo Stato procedente.

Tale norma ha destato molte perplessità nel corso del negoziato, poiché attribuiva al prestatore di servizi un singolare ruolo di garante degli interessi politici del paese terzo (in fin dei conti soprattutto di quello in cui il *provider* aveva la propria sede di stabilimento, spesso coincidente con gli Stati Uniti), conferendogli di fatto il potere di bloccare temporaneamente l'esecuzione di un ordine giudiziario sulla base di valutazioni totalmente discrezionali che non gli competevano. Inoltre, finiva comunque per subordinare alla decisione del paese terzo la sorte dell'ordine di produzione, imponendo allo stesso tempo una procedura macchinosa e lenta, incompatibile con la volatilità del dato elettronico. L'articolo 15, pertanto, è stato totalmente eliminato dal Consiglio UE in sede di orientamento generale.

È sopravvissuto invece l'articolo 16, che è stato tuttavia modificato nel senso di prevedere un'unica procedura di riesame che il *service provider* può attivare, entro dieci giorni dal ricevimento dell'ordine di acquisizione, in tutti i casi in cui rilevi che l'ottemperanza si pone in conflitto con la legge di un paese terzo. In tal caso deve informarne l'autorità emittente utilizzando il modulo contenuto nell'allegato III della proposta di Regolamento ed indicando i motivi per i quali ritiene che sussistano obblighi contrastanti: si applica a quel punto la procedura prevista dall'articolo 9(5) e (6) dell'orientamento generale per notificare l'intenzione di non ottemperare all'EPOC.

Sulla base dell'obiezione motivata del *provider* l'autorità di emissione rivede il proprio ordine. È importante evidenziare che la motivazione non può fondarsi sul mero fatto che il diritto del paese terzo non prevede disposizioni analoghe, né sulla sola circostanza che i dati sono conservati in un paese terzo. Se l'autorità emittente decide di ritirare l'ordine, la procedura si conclude. Se invece intende confermarlo, investe del caso l'autorità giurisdizionale competente del proprio Stato e ciò sospende

temporaneamente l'esecutività dell'ordine fino al termine della procedura di riesame. Il giudice in questione è chiamato, quindi, a valutare, tenuto conto di tutte le circostanze del caso, se il diritto del paese terzo si applica al caso di specie e, in caso affermativo, se sussistono effettivamente obblighi contrastanti. *Può*, a tal fine, chiedere informazioni all'autorità competente del paese terzo, nella misura in cui ciò non crei pregiudizi alle indagini. Se conclude che esiste un contrasto, al fine di decidere se confermare o ritirare l'ordine di acquisizione deve tenere in conto le circostanze previste dal comma 5 dell'articolo 16 dell'orientamento generale, attribuendo una valenza particolare all'interesse protetto dalla legge del paese terzo (ivi inclusa la necessità di tutela di diritti fondamentali o di altri interessi, in particolare di sicurezza nazionale del paese terzo, che impediscano la consegna dei dati) e al grado di connessione del procedimento penale con la giurisdizione di nazionalità, di residenza o dimora del soggetto a cui i dati appartengono o delle vittime del reato, ovvero con la giurisdizione del luogo di consumazione del reato. Ove l'autorità giurisdizionale si esprima nel senso della conferma dell'ordine di acquisizione già emesso, ne informa l'autorità di emissione dell'ordine e il rappresentante legale del prestatore di servizi, che è tenuto a quel punto ad adempiere: il Consiglio UE ha, pertanto, eliminato il carattere obbligatorio e vincolante della consultazione dello Stato terzo contemplato dalla proposta originaria della Commissione, prevedendo altresì l'obbligo del destinatario di dare esecuzione all'ordine in caso di sua conferma da parte delle autorità dello Stato di emissione all'esito della procedura di riesame.

Nonostante gli sforzi di semplificazione posti in essere durante il negoziato, l'articolo 16 dell'orientamento generale non è apparso sufficiente agli Stati membri a disciplinare in maniera coerente ed efficace i conflitti tra l'adottando Regolamento e la legislazione dei paesi terzi, soprattutto quella degli Stati Uniti che ospitano la maggior parte dei *service providers*. Il possibile rimedio è stato individuato nella conclusione di accordi internazionali bilaterali sull'accesso transfrontaliero alle prove elettroniche tra l'UE e i paesi terzi dove abbiano sede di stabilimento i prestatori di servizi, iniziando proprio dagli Stati Uniti. Questi ultimi, peraltro, il 23 marzo 2018 hanno adottato una normativa in tema di acquisizione della prova elettronica, il *CLOUD Act (Clarifying Lawful Overseas Use of Data Act – H.R. 4943)*[24], che subordina alla conclusione di tali accordi la possibilità per i *providers* statunitensi di consegnare i dati di *soggetti non statunitensi* richiesti da autorità non nazionali. Nella stessa direzione va, peraltro, la normativa dell'Unione in materia di protezione dei dati personali, secondo cui "le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento [e quindi anche di un *service provider*] possono essere riconosciute o assumere qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione [...], fatti salvi altri motivi di trasferimento a norma del capo [V]" (articolo 48 del Regolamento generale UE sulla protezione dei dati n. 2016/679).

[24] Si rimanda al testo del *CLOUD Act* reperibile sul sito del Congresso statunitense al seguente *link*.

Alla luce di tali rilievi ed in considerazione del principio di reciprocità che governa le relazioni internazionali, i Ministri della Giustizia degli Stati membri hanno già più volte espresso, in sede di Consiglio UE, favore unanime per avviare il negoziato di un accordo bilaterale UE – Stati Uniti in parallelo con i lavori legislativi sulla proposta di Regolamento, al fine di accelerare i tempi ed assicurare la massima coerenza possibile tra i due strumenti. Tale negoziato, secondo i Trattati UE, dovrebbe essere condotto dalla Commissione europea in virtù della competenza esclusiva dell'Unione in materia, sulla base di un mandato negoziale conferitole dal Consiglio UE. Al riguardo, tuttavia, sembrano persistere dei nodi da sciogliere tra i quali l'ambito da attribuire al mandato negoziale della Commissione, affinché sia compatibile con la previsione del *CLOUD Act* statunitense che regola gli accordi esecutivi con i Governi stranieri per consentirne l'accesso diretto ai dati custoditi dai prestatori di servizi statunitensi (paragrafo 2523). In particolare, la norma statunitense prevede che vi sia una valutazione positiva da parte delle competenti autorità degli Stati Uniti in merito alla rilevante normativa sostanziale e processuale di *ciascun* paese straniero con cui si vuole concludere l'accordo (soprattutto quella in materia di tutela dei diritti umani e dei dati personali e sul *cybercrime*) e ciò renderebbe, pertanto, necessario, ai sensi del *CLOUD Act*, che ogni singolo Stato membro dell'Unione firmi un accordo con gli U.S.A. che tenga conto del proprio quadro normativo interno, non potendo pertanto concludersi un unico strumento convenzionale tra Unione europea e Stati Uniti. Una possibile soluzione a questo problema sarebbe quella di stipulare un accordo quadro (*framework agreement*) tra UE e U.S.A. – come peraltro già avvenuto per l'accordo sulla mutua assistenza giudiziaria del 2009[25] – che costituisca una sorta di ombrello generale basato sul comune *acquis* normativo europeo, al di sotto del quale dovrebbero essere poi firmate – in maniera più rapida e per i soli aspetti non compresi nell'accordo quadro – le singole convenzioni da parte di ogni Stato membro. È, tuttavia, di chiara evidenza che anche questa soluzione finirebbe con l'allungare notevolmente i tempi per giungere a misure condivise con gli Stati Uniti.

Peraltro, non può non rilevarsi che le criticità rogatoriali registratesi con gli U.S.A. per la conservazione e l'acquisizione della prova elettronica dai prestatori di servizi ivi stabiliti sembrano ormai attenere alla sola acquisizione dei dati più sensibili, ovvero quelli relativi alle operazioni e al contenuto, per i quali la legge statunitense impone l'emissione di un provvedimento di acquisizione da parte del giudice U.S.A. ("*warrant*") anche ove la richiesta venga formulata per via di cooperazione giudiziaria da uno stato terzo. Ormai pacificamente, invece, le autorità giudiziarie europee possono accedere ai dati relativi agli abbonati e agli accessi o chiederne la conservazione al *provider* statunitense senza attivare un meccanismo rogatoriale, ma formulando una semplice richiesta diretta al prestatore di servizi: il formato o i moduli di tali richieste sono, peraltro, messi a disposizione dagli stessi *providers* su apposite pagine *web* dei loro

[25] Decisione 2009/820/PESC del Consiglio del 23 ottobre 2009, relativa alla conclusione, a nome dell'Unione europea, dell'accordo sull'estradizione tra l'Unione europea e gli Stati Uniti d'America e dell'accordo sulla mutua assistenza giudiziaria tra l'Unione europea e gli Stati Uniti d'America.

siti dedicate alle relazioni con le autorità giudiziarie e le forze dell'ordine[26] (per esempio, da Facebook e da WhatsApp).

La questione che dal punto di vista investigativo dell'Unione europea rimane, pertanto, decisiva da risolvere è la consegna dei dati attinenti alle operazioni ed al contenuto rispetto alla quale, tuttavia, la procedura di riesame sopravvissuta nell'articolo 16 dell'orientamento generale appare come un "cavallo di Troia" nell'impianto e nella logica complessiva del Regolamento. Se la finalità dell'Unione è, infatti, quella di obbligare il *service provider* che sia stabilito in un paese terzo a nominare un proprio rappresentante legale nel territorio europeo, affinché possa essere destinatario di ordini di acquisizione e conservazione della prova elettronica a cui deve ottemperare indipendente dal luogo della propria sede principale di stabilimento e dal luogo di conservazione dei dati, per la semplice ragione che presta i propri servizi in Europa, allora non si vede come possa conferirsi una valenza potenzialmente ostativa al conflitto di obblighi rispetto alla legislazione dello stato terzo in cui è principalmente stabilito. Così come il *CLOUD Act* statunitense ha previsto che il *provider* stabilito negli Stati Uniti debba consegnare i dati richiesti dall'autorità giudiziaria statunitense *indipendentemente dal luogo di conservazione di tali dati* (vedasi paragrafo 2713[27]), ugualmente l'Unione europea dovrebbe obbligare il rappresentante legale del *provider* sul proprio territorio (eventualmente imponendone un obbligo di stabilimento se necessario), a consegnare i dati per esigenze di giustizia e di sicurezza dei cittadini europei. Non a caso il *CLOUD Act* prevede una procedura di riesame dell'ordine di acquisizione che può essere attivata dal prestatore di servizi stabilito negli Stati Uniti innanzi all'autorità giudiziaria statunitense ("*comity analysis*") per confliggenti obblighi con la legislazione di uno paese terzo *solo* nel caso in cui già sussista un accordo bilaterale con quel paese terzo (*"qualifying foreign government"*) e si tratti di dati relativi ad un soggetto non statunitense (come già detto, ai dati dei soggetti statunitensi non sono applicabili gli accordi esecutivi conclusi con i paesi terzi)[28]: la procedura in parola sembra

---

[26] In particolare, non occorre che l'autorità competente degli Stati membri esperisca una rogatoria verso gli Stati Uniti nei seguenti casi:
– Chiedere il congelamento dei contenuti dell'*account*. L'autorità inquirente o la polizia giudiziaria possono chiedere la conservazione dei dati per un periodo fino a 180 giorni, accedendo direttamente alle pagine *web* dedicate dai *providers* alle relazioni con le forze dell'ordine.
– Ottenere i dati anagrafici dell'intestatario dell'*account*. L'autorità inquirente o la polizia giudiziaria possono chiedere questi dati tramite le pagine *web* sopra menzionate.
– Ottenere i dati di accesso dell'utente (i cosiddetti "*access logs*," ad esempio, dati, orari, indirizzi IP associati a ciascun accesso dell'utente). L'autorità inquirente può chiedere questi dati tramite le pagine *web* sopra menzionate.

[27] *§2713. Required preservation and disclosure of communications and records:"A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."*

[28] Riguardo alla procedura di riesame attivabile dal *provider*, nel paragrafo 2713 del *CLOUD Act* si legge: *"(2) MOTIONS TO QUASH OR MODIFY— (A) A provider of electronic communication service to the public or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process*

pertanto costituire più una forma di garanzia della corretta esecuzione della convenzione internazionale con il paese terzo, che una procedura generale di ricorso come invece quella prevista dall'articolo 16 dell'orientamento generale del Consiglio UE.

Ove si riuscisse normativamente a costruire nel nuovo Regolamento un obbligo per il *provider* così articolato, eliminando la procedura di riesame di cui all'articolo 16 o limitandola alla funzione prevista dalla corrispondente *"comity analysis"* del *CLOUD Act*, non vi sarebbe probabilmente bisogno neanche di un accordo bilaterale U.S.A.-UE ai fini del rispetto del paragrafo 2523 del *CLOUD Act* e dell'articolo 48 del Regolamento Generale UE sulla protezione dati, atteso che tali norme si applicano entrambe al solo caso dell'esecuzione del provvedimento di un'autorità straniera, laddove l'ordine europeo di produzione sarebbe invece un provvedimento giudiziario emesso nello spazio unico europeo di giustizia nei confronti di una società commerciale avente sede di stabilimento/rappresentanza legale nel territorio dell'Unione. Ciò dovrebbe rendere irrilevante il fatto che essa abbia *anche* un'altra sede di stabilimento in un paese terzo. Il

---

where the provider reasonably believes:
"(i) that the customer or subscriber is not a United States person and does not reside in the United States; and
"(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.
Such a motion shall be filed not later than 14 days after the date on which the provider was served with the legal process, absent agreement with the government or permission from the court to extend the deadline based on an application made within the 14 days. The right to move to quash is without prejudice to any other grounds to move to quash or defenses thereto, but it shall be the sole basis for moving to quash on the grounds of a conflict of law related to a qualifying foreign government.
"(B) Upon receipt of a motion filed pursuant to subparagraph (A), the court shall afford the governmental entity that applied for or issued the legal process under this section the opportunity to respond. The court may modify or quash the legal process, as appropriate, only if the court finds that:
"(i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government;
"(ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and
"(iii) the customer or subscriber is not a United States person and does not reside in the United States.
"(3) COMITY ANALYSIS. — For purposes of making a determination under paragraph (2)(B)(ii), the court shall take into account, as appropriate:
"(A) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;
"(B) the interests of the qualifying foreign government in preventing any prohibited disclosure;
"(C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider;
"(D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country;
"(E) the nature and extent of the provider's ties to and presence in the United States;
"(F) the importance to the investigation of the information required to be disclosed;
"(G) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and
"(H) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance.

problema che, invece, permarrebbe in termini di garanzia del soggetto i cui dati vengano richiesti è quello dell'esistenza di limiti legislativi nazionali o internazionali derivanti da immunità, privilegi o attinenti alla professione svolta, rispetto ai quali sembrano tuttavia già sufficienti le protezioni apprestate dalla procedura di notifica all'autorità competente dello Stato membro di esecuzione dell'ordine di acquisizione prevista da nuovo articolo 7a dell'orientamento generale ed i limiti di utilizzo probatorio dei dati nel procedimento penale stabiliti dal nuovo articolo 12a di cui abbiamo trattato in precedenza.

4. Conclusioni.

Il quadro normativo che emerge dall'orientamento generale adottato il 7 dicembre 2018 dal Consiglio dell'Unione europea sulla proposta di Regolamento della Commissione che istituisce gli ordini europei di produzione e conservazione della prova elettronica appare, per molti versi, più un punto di partenza che un punto di arrivo. Come si evince dalle riflessioni finora svolte, molti sono ancora gli aspetti critici che dovranno essere affrontati nel negoziato di trilogo tra la Commissione, il Consiglio ed il Parlamento europeo in vista dell'adozione degli strumenti normativi di cui ci siamo occupati, tra cui particolarmente controversa appare la decisione sulla valenza da attribuire alla notifica dell'ordine di produzione allo Stato di esecuzione ed in particolare sul se mantenerne una natura meramente informativa (come attualmente previsto) oppure – come vorrebbero taluni Stati membri, finora in minoranza – farla divenire un mezzo di sindacato effettivo e di eventuale opposizione dal parte dello Stato di esecuzione. La risposta dipenderà dal grado di reale volontà degli Stati membri di dare piena applicazione al principio del mutuo riconoscimento delle decisioni giudiziarie nazionali, che è strettamente collegato alla disponibilità a rinunciare alla propria sovranità nazionale ai fini della concreta realizzazione di uno spazio unico di libertà, giustizia e sicurezza. Tema delicato questo, soprattutto in un momento in cui si registra una generale tendenza degli Stati a chiudersi nella sfera della propria sovranità nazionale, ma rispetto al quale un contributo importante potrebbe essere dato dal Parlamento europeo, che spesso nell'esercizio della sua funzione di co-legislatore ha dato prova di saper promuovere il raggiungimento di traguardi più ambiziosi rispetto a quelli proposti dagli Stati membri, guardando alla realizzazione di una effettiva integrazione giuridica europea.

L'altro nodo essenziale che dovrà essere affrontato sarà quello del negoziato dell'accordo tra l'Unione e gli Stati Uniti di cui abbiamo parlato, rispetto al quale sarà necessario un approfondimento e un chiarimento delle finalità che si vogliono raggiungere e degli *effettivi* ambiti di incompatibilità delle normative di riferimento, al fine di evitare l'introduzione di macchinose procedure di riesame destinate ad ostacolare le attività di contrasto alla criminalità organizzata e al terrorismo che rientrano negli obiettivi politici primari di tutti gli Stati da un lato e dall'altro dell'Oceano.

Infine, non può concludersi che con un auspicio: che i prossimi lavori negoziali che si terranno nel 2019 sotto Presidenza rumena consentano di migliorare le iniziative legislative che abbiamo esaminato nel senso di potenziarne la concreta utilità

investigativa. A tal fine, molto dipenderà dalla capacità politica dell'Unione di far valere nei confronti dei prestatori di servizi la prioritaria esigenza di acquisizione della *e-evidence* per ragioni di giustizia e di sicurezza dei cittadini, soprattutto con riferimento all'esigenza di ottenere *sempre* la consegna di dati leggibili in chiaro, indipendentemente dal sistema di criptazione utilizzato: istanza che finora è apparsa purtroppo spesso recessiva rispetto agli interessi economici ed imprenditoriali di questi colossi del mercato.