5/2018

LOTTA ALLA CRIMINALITÀ NEL CYBERSPAZIO: LA COMMISSIONE PRESENTA DUE PROPOSTE PER FACILITARE LA CIRCOLAZIONE DELLE PROVE ELETTRONICHE NEI PROCESSI PENALI

di Mitja Gialuz e Jacopo Della Torre (*)

Abstract. *Il testo analizza le genesi e i contenuti di due importanti proposte normative, recentemente presentate – dopo un lungo periodo di gestazione – dalla Commissione europea, al fine di rendere più efficiente la circolazione delle prove elettroniche nei procedimenti penali all'interno dello spazio di libertà, sicurezza e giustizia.*

1. Prodromi.

«Le prove elettroniche sono sempre più importanti nei procedimenti penali. Non possiamo permettere che i criminali e i terroristi sfruttino le moderne tecnologie di comunicazione […] per occultare le loro azioni criminali e sottrarsi alla giustizia»[1]. Con queste parole il primo Vicepresidente della Commissione europea ha presentato, il 17 aprile scorso, un importante pacchetto di interventi[2] – di cui fanno parte una proposta

(*) Pur essendo frutto di una riflessione comune, i §§ 1-3 sono stati redatti da Mitja Gialuz, mentre i §§ 3.1-5 da Jacopo Della Torre.

[1] Così, Commissione europea – Comunicato stampa, *Unione della sicurezza: la Commissione facilita l'accesso alle prove elettroniche*, IP/18/3343.

[2] Cfr. *Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo e al Consiglio. Fourteenth progress report towards an effective and genuine Security Union*, COM (2018) 211 final, § II. Per una prima presentazione delle due proposte legislative della Commissione, cfr. J.-H. JEPPESEN – G. NOJEIM, *Initial Observations on the European Commission's E-Evidence Proposals*, in www.cdt.org, 18 aprile 2018; L. MOXLEY, *EU Releases e-Evidence Proposal for Cross-Border Data Access*, in www.insideprivacy.com, 8 maggio 2018. In lingua italiana, cfr. B. ROMANO, *I big tech dovranno fornire dati ai magistrati di altri Paesi Ue*, in

di Regolamento[3] e una di Direttiva[4] – vòlto a semplificare la circolazione transfrontaliera delle prove digitali[5] nei procedimenti penali all'interno dello spazio di libertà, sicurezza e giustizia (SLSG).

Si tratta di un'iniziativa fortemente voluta da tutte le più importanti istituzioni europee, che si colloca all'esito di un lungo percorso. I primi passi risalgono al 2015, quando nella sua Agenda sulla sicurezza la Commissione aveva rilevato l'«importanza fondamentale» della tematica della «raccolta delle prove elettroniche [...] da altre giurisdizioni»[6].

Una vera e propria svolta si è registrata a seguito degli attentati di Bruxelles del marzo del 2016: nella dichiarazione congiunta dei ministri della giustizia e degli interni per il Consiglio GAI e dei rappresentanti delle altre istituzioni UE su tali tragici fatti si è posta in rilievo l'importanza prioritaria di «trovare […] modalità per assicurare e ottenere più rapidamente ed efficacemente prove digitali, intensificando la cooperazione con i paesi terzi e con i fornitori di servizi operanti nel territorio europeo»[7].

Nell'aprile 2016, la Commissione ha quindi dichiarato di voler trovare una soluzione per tale problematica, anche mediante uno strumento giuridico da presentare già nel 2017[8]. All'interno delle sue Conclusioni sul miglioramento della giustizia penale nel cyberspazio il Consiglio UE ha supportato tale iniziativa, invitando direttamente la Commissione ad agire[9]. Come di consueto, quest'ultima ha iniziato un processo di consultazione dei maggiori *stakeholders* nazionali[10] (industrie, fornitori di servizi internet,

---

www.ilsole24ore.com, 17 aprile 2018.

[3] Cfr. *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.

[4] V. *proposta di Direttiva del Parlamento europeo e del Consiglio, recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali*, COM (2018) 226 final.

[5] Per i dovuti riferimenti dottrinali in merito alla spinosa tematica delle "prove digitali", si rimanda, per tutti, a M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, p. 283 ss.; L. LUPÁRIA (a cura di), Internet provider *e giustizia penale: modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012; ID., *Sistema penale e criminalità informatica: profili sostanziali e processuali della Legge attuativa della Convenzione di Budapest sul* cybercrime, Milano, 2009; ID. – G. ZICCARDI, *Investigazione penale e tecnologia informatica: l'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007; L. MARAFIOTI, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, p. 4509 ss.; F. RUGGIERI – L. PICOTTI (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018; EAD., *Types and Features of Cyber Investigations in a Globalized World*, in *Dir. pen. cont. – Riv. trim.*, 3/2016, p. 194 ss.

[6] Cfr. *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni*, COM (2015) 185 final, § 3.3.

[7] V. *Dichiarazione comune dei ministri della giustizia e degli interni dell'UE e dei rappresentanti delle istituzioni dell'UE sugli attentati terroristici di Bruxelles del 22 marzo 2016*, disponibile al questo *link*.

[8] Cfr. *Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo e al Consiglio. Attuare l'Agenda europea sulla sicurezza per combattere il terrorismo e preparare il terreno per l'Unione della sicurezza*, COM (2016) 230 final, § 2.3. Si veda, effettivamente, la *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni. Programma di lavoro della Commissione per il 2017. Realizzare un'Europa che protegge, dà forza e difende*, COM (2016) 710 final, § 7.

[9] V. *Conclusioni del Consiglio UE, sul miglioramento della giustizia penale nel cyberspazio*, del 9 giugno 2016.

[10] I risultati della consultazione sono disponibili a questo *link*.

rappresentanti di organizzazioni governative e non governative e accademici) e ha pubblicato diversi documenti preparatori preliminari[11].

Nel corso del 2017 un'accelerazione ulteriore dei lavori è stata determinata dal Consiglio europeo, il quale ha espressamente affermato, tra l'altro, che «l'effettivo accesso alle prove elettroniche [è] essenziale per combattere le gravi forme di criminalità e il terrorismo»[12].

A seguito di tali stimoli, il Consiglio[13] e il Parlamento UE[14] hanno ripetutamente invitato la Commissione ad agire e, dal canto suo, il Presidente Juncker ha annunciato che la Commissione sarebbe stata pronta a presentare una proposta legislativa ufficiale in materia di *electronic evidence* nel 2018[15].

Sulla scorta di tali considerazioni, non stupirà che, nel dicembre 2017, l'iniziativa in materia di circolazione delle prove digitali sia stata inserita nella dichiarazione congiunta del Parlamento, Consiglio e Commissione sulle priorità legislative UE per il periodo 2018-2019[16], da approvare possibilmente «*before the European elections of 2019*»[17].

2. Le ragioni dell'intervento dell'Unione.

Le ragioni per cui le istituzioni UE si sono dimostrate concordi circa l'urgenza di un intervento in materia di circolazione transnazionale delle prove digitali sono state esplicitate in molteplici atti, tra cui spicca *l'Impact Assessment* che accompagna il pacchetto di interventi in commento[18].

---

[11] Si vedano, ad esempio, l'*Inception Impact Assessment*, *Improving cross-border access to electronic evidence in criminal matters*, Ref. Ares. 2017 3896097 - 03/08/2017 e il *Non-paper*, *Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward*, disponibile a questo *link*.

[12] Cfr. *Conclusioni del Consiglio europeo del 22 e 23 giugno 2017*, EUCO 8/17, § I, 2. V. anche le *Conclusioni del Consiglio europeo del 19 ottobre 2017*, EUCO 14/17.

[13] Durante la riunione del Consiglio dell'8-9 giugno 2017 i ministri hanno sostenuto, a grande maggioranza, che «occorre esaminare l'eventualità di un'iniziativa legislativa dell'UE riguardo alla cooperazione diretta con i fornitori di servizi e alla definizione di condizioni comuni e requisiti minimi in ambito UE per l'accesso diretto ai dati da parte delle autorità a partire da un sistema informatico». Si veda sul punto il seguente link: http://www.consilium.europa.eu/it/meetings/jha/2017/06/08-09/. Cfr. anche *Documento del Consiglio UE 14435/17*, del 20 novembre 2017; *Documento del Consiglio UE, 15748/17*, del 12 dicembre 2017.

[14] Ci si riferisce alla *Risoluzione del Parlamento europeo del 3 ottobre 2017 sulla lotta alla criminalità informatica* (2017/2068/INI).

[15] Si veda la lettera di intenti, *State of the Union 2017. Letter of intent to President Antonio Tajani and to Prime Minister Jüri Ratas*, del 13 settembre 2017, p. 9. Cfr. anche la *Comunicazione congiunta della Commissione al Parlamento europeo e al Consiglio, Resilienza, deterrenza e difesa: verso una cirbersicurezza forte per l'UE*, JOIN (2017) 450 final, p. 15.

[16] Cfr. Commissione europea, *Working document for the Joint Declaration on the EU's legislative priorities for 2018-19, 31 new initiatives for a More United, Stronger and More Democratic Union*.

[17] Così, *Comunicazione congiunta dei Presidenti del Parlamento europeo, del Consiglio e della Commissione, on the EU's legislative priorities for 2018-19*, p. 1.

[18] Cfr. *Commission staff working document, Impact Assessment*, SWD (2018) 188 final. Per una sintesi si veda il documento SWD (2018) 119 final.

Questa scelta di politica normativa è giustificata anzitutto da un dato empirico: secondo i dati raccolti dalla Commissione, più della metà delle investigazioni penali svolte nello SLSG necessiterebbero oggi di una richiesta transnazionale di accesso a materiale probatorio elettronico[19]. È del resto noto che le prove digitali – quali, ad esempio, i messaggi inoltrati via WhatsApp, e-mail o Facebook – si trovano spesso «*in the cloud, on a server in another country and/or held by service providers that are located in other countries*»[20]. Come ricordato, i recenti attacchi terroristici avvenuti in Europa hanno poi reso la situazione ancora più delicata: l'esperienza pratica dimostra che, per contrastare tale odiosa forma di criminalità, è essenziale un'efficiente circolazione delle prove digitali nell'Unione[21].

Tuttavia, gli strumenti ufficiali di cooperazione giudiziaria finora esistenti, vòlti a consentire la trasmissione di prove elettroniche tra Stati membri, oppure tra uno Stato terzo e uno UE[22], sono stati considerati del tutto inadeguati dalle istituzioni eurounitarie[23]. Si è infatti affermato che la Direttiva 2014/41/UE sull'ordine europeo di indagine penale (OEI)[24] e i meccanismi di mutua assistenza giudiziaria (bilaterali o multilaterali) con Stati terzi richiedono tempi troppo lunghi affinché la richiesta di una prova informatica vada a buon fine[25]. Tali mezzi sarebbero quindi sostanzialmente inefficaci, considerata la grande rapidità con cui i dati digitali possono essere occultati o comunque trasferiti altrove. Senza contare poi che alcuni Stati chiave come l'Irlanda, in cui sono allocati alcuni tra i più importanti *providers* che forniscono servizi informatici nell'Unione, non partecipano neppure all'OEI[26].

Una forte critica ai meccanismi giudiziali esistenti di raccolta delle prove digitali all'estero proviene anche dal *Cybercrime Convention Committee*[27], costituito sulla base dell'art. 46 della Convenzione di Budapest del Consiglio d'Europa sulla criminalità

---

[19] V. *Impact Assessment*, cit., p. 14, ove si afferma, testualmente, che «*more than half of all investigations include a cross-border request to access e-evidence*». Più in generale, sulla "transnazionalità" delle prove digitali, cfr. la compiuta analisi di S. SIGNORATO, *Le indagini digitali*, cit., pp. 152 ss.

[20] Così, il documento della Commissione europea, *Security Union. Facilitating access to electronic evidence*, April 2018, disponibile a questo *link*.

[21] Si veda, solo a scopo esemplificativo, la fattispecie riportata dall'*Impact Assessment*, cit., p. 18.

[22] Per un quadro dei quali, cfr. S. SIGNORATO, *Le indagini digitali*, cit., pp. 167 ss.

[23] V. *Impact Assessment*, cit., p. 9 ss.

[24] Sul rapporto tra OEI e prove elettroniche cfr. S. SIGNORATO, *Le indagini digitali*, cit., pp. 173 ss. Più in generale, per i dovuti riferimenti dottrinali sulla Direttiva 2014/41/UE, si vedano G. BARROCU, *La cooperazione investigativa in ambito europeo. Da Eurojust all'ordine di indagine*, Padova, 2017, p. 191 ss.; T. BENE – L. LUPÁRIA – L. MARAFIOTI (a cura di), *L'ordine europeo di indagine: criticità e prospettive*, Torino, 2016; L. CAMALDO, *La normativa di attuazione dell'ordine europeo di indagine penale: le modalità operative del nuovo strumento di acquisizione della prova all'estero*, in *Cass. pen.*, 2017, p. 4196 ss.; M. DANIELE, *L'impatto dell'ordine europeo di indagine penale sulle regole probatorie nazionali*, in *Dir. pen. cont. – Riv. trim.*, 3/2016, p. 63 ss.; ID., *Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles*, in *New Journal of European Criminal Law*, 2015, p. 179 s.

[25] Cfr. *Impact Assessment*, cit., p. 23.

[26] Sul punto, *Impact Assessment*, cit., p. 23.

[27] Cfr. *T-CY Assessment Report, The mutual legal assistance provisions of the Budapest Convention on Cybercrime, Adopted by the T-CY at its 12th Plenary (2-3 December 2014)*, Strasbourg, p. 123.

informatica[28]. Pure tale istituzione ha infatti affermato, per un verso, che l'attuale sistema di circolazione transnazionale delle evidenze elettroniche è troppo lento e, per altro verso, che gli Stati parti della Convenzione europea sul *cybercrime* «*appear not to make full use of the opportunities offered by the Budapest Convention*»[29].

Proprio in ragione dei ritardi dovuti agli strumenti di cooperazione giudiziaria ufficiali, le autorità nazionali hanno iniziato a contattare direttamente i *service providers* situati in altri Stati (appartenenti all'Unione o terzi), senza passare per il tramite delle autorità del Paese di esecuzione, instaurando così canali di comunicazione del materiale probatorio elettronico costruiti su base "volontaria"[30]. Neppure questa via alternativa (e più rapida) di accesso alle prove digitali[31] è stata però considerata soddisfacente dalle istituzioni dell'Unione. In mancanza di regole comuni europee, la cooperazione diretta tra autorità nazionali e fornitori di servizi internet «*may generate legal uncertainty*» e risulta critica «*as well as concerns on the protection of fundamental rights and procedural safeguards for the persons related to such requests*»[32]. Difatti, gli Stati membri si sono finora approcciati alla cooperazione diretta con i *service providers* «ricorrendo a strumenti, condizioni e procedure nazionali diversi»[33], dando così vita a un quadro normativo alquanto frammentato[34], che ha creato notevoli difficoltà operative agli stessi fornitori di servizi[35].

Secondo la Commissione, tutto ciò ha ingenerato un circolo vizioso: nello spazio di libertà, sicurezza e giustizia meno della metà delle richieste probatorie ai *service providers* hanno oggi effettivamente esito positivo[36], di modo che almeno due-terzi dei reati, che necessiterebbero di prove digitali raccolte all'estero, non possono essere perseguiti efficacemente[37].

Alla luce di questi dati allarmanti, non stupiranno le parole con cui la Commissaria alla giustizia Věra Jourová ha riassunto la logica del pacchetto di intervento in esame: «mentre le autorità di contrasto continuano a lavorare con metodi gravosi, i criminali operano usando tecnologie veloci e all'avanguardia. Come i criminali, anche le autorità di contrasto devono poter ricorrere a metodi propri del 21º secolo per combattere la criminalità»[38].

---

[28] STE n. 185. Sulla quale cfr., per tutti, L. LUPÀRIA, *La ratifica della Convenzione CyberCime del Consiglio d'Europa. I profili processuali*, in *Dir. pen. proc.*, 2008, p. 720-723.

[29] *T-CY assessment report, The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, cit., p. 123.

[30] Cfr. *Impact Assessment*, cit., p. 26. Pare utile precisare che, in questo contesto, "volontario" «*means that there is a domestic legal title which cannot be enforced directly in the recipient country*» (*ibidem*, nt. 37).

[31] Sul ruolo centrale giocato da soggetti terzi, come i fornitori di servizi, nelle indagini informatiche si vedano le riflessioni di S. SIGNORATO, *Le indagini digitali*, cit., pp. 181 ss.

[32] Cfr. *Impact Assessment*, cit., p. 5, da cui è tratta anche la citazione immediatamente precedente.

[33] Si veda sul punto il considerando 8 della *proposta di Regolamento*.

[34] Cfr. considerando 6 della *proposta di Regolamento*.

[35] Si veda la *proposta di Direttiva*, cit., p. 7.

[36] In questo senso, *Impact Assessment*, cit., p. 15.

[37] V. *Impact Assessment*, cit., p. 17.

[38] Così, Commissione europea – Comunicato stampa, *Unione della sicurezza*, cit., p. 1.

3. La proposta di Regolamento UE sull'ordine di produzione e di conservazione europeo delle prove elettroniche.

Nei suoi documenti preparatori la Commissione europea ha messo a confronto diverse ipotesi di intervento per risolvere le criticità degli strumenti di cooperazione vigenti in materia di *e-evidence*[39]. L'opzione alla fine prescelta mira a regolare i casi e i modi in cui le autorità nazionali possono rivolgersi direttamente ai *service providers*[40], che operano nello SLSG (anche se la loro sede centrale è allocata in un Paese terzo[41]), per ottenere o far conservare il materiale probatorio digitale di cui necessitano[42]. L'Unione ha quindi deciso di puntare sulla cooperazione diretta tra soggetti pubblici e fornitori di servizi internet, manifestando oltretutto il proposito di stabilire un corposo apparato di garanzie processuali, volte ad assicurare il pieno rispetto dei diritti fondamentali dei soggetti coinvolti nella procedura[43].

Evidentemente, si tratta di un approccio basato su un alto livello di fiducia reciproca tra Stati membri[44], il quale risulta indispensabile per il buon funzionamento di un meccanismo che, di norma, non richiede il coinvolgimento di un'autorità giudiziaria del Paese di esecuzione della misura. Esso però va salutato in modo alquanto positivo, perché consentirà finalmente ai *service provider* di cooperare in materia di prove elettroniche in un quadro giuridico chiaro e non frammentario[45].

Come anticipato, questi obiettivi di fondo sono perseguiti tramite la presentazione di un pacchetto normativo composto da due atti legislativi.

Il provvedimento principale è rappresentato da un'assai articolata proposta di Regolamento – la cui base giuridica è individuata nell'art. 82, par. 1, TFUE[46] – volta a istituire due nuovi "ordini europei": l'ordine europeo di produzione (OPE) e di conservazione (OCE) delle prove elettroniche nei procedimenti penali.

Tale iniziativa si compone allo stato di ben 66 considerando e 25 articoli, suddivisi in cinque capi.

---

[39] V. *Impact Assessment*, cit., p. 41 ss.

[40] Cfr. il considerando 9 della *proposta di Regolamento*, dove si afferma che «occorre pertanto presentare un quadro giuridico europeo in materia di prove elettroniche che imponga ai prestatori di servizi che rientrano nell'ambito di applicazione dello strumento di rispondere direttamente alle autorità, senza che sia necessario l'intervento di un'autorità giudiziaria nello Stato membro del prestatore di servizio».

[41] Cfr. Commissione europea – Comunicato stampa, *Unione della sicurezza*, cit., p. 2.

[42] Cfr. *proposta di Regolamento*, cit., p. 13.

[43] Si veda la *proposta di Regolamento*, cit., p. 2, dove si afferma che i nuovi strumenti «sono subordinati alla condizione di essere soggetti a forti meccanismi di tutela dei diritti fondamentali».

[44] Cfr. il considerando 11 della *proposta di Regolamento*.

[45] V. il considerando 9 della *proposta di Regolamento*.

[46] Cfr. la *proposta di Regolamento*, cit., p. 5 s.

3.1. Capo I: oggetto, definizioni e ambito di applicazione.

Il Capo I (artt. 1-3, considerando 1-27)[47] racchiude alcune delle previsioni più importanti dell'intero testo: esso stabilisce infatti l'oggetto dell'atto, il suo ambito di operatività e tutta una serie di definizioni fondamentali.

In estrema sintesi, il Regolamento dovrebbe applicarsi:

a) alle situazioni transfrontaliere, non avendo invece a oggetto fattispecie puramente interne (considerando 15 e art. 1);

b) nelle sole ipotesi in cui un'autorità di uno Stato membro chieda, nel corso di un procedimento penale già avviato[48] avverso una persona fisica o giuridica[49], a un *service provider* la consegna o la conservazione di prove elettroniche[50] esistenti e non per l'intercettazione in tempo reale di dati informatici (considerando n. 19);

c) a tutti i *provider* – persone fisiche o giuridiche[51] – che offrano nel territorio dell'Unione i servizi stabiliti all'art. 2, par. 3, della proposta, indipendentemente dal fatto che gli stessi abbiano la loro sede centrale in un Paese terzo[52] e da dove siano ubicati i dati[53].

L'art. 2 della proposta fornisce poi un elenco di definizioni di tutta una serie di concetti chiave utilizzati nel testo. Tale disposizione precisa, ad esempio, che per "ordine di produzione europeo" bisogna intendersi una «decisione vincolante di un'autorità di emissione di uno Stato membro che ingiunge a un prestatore di servizi […] di produrre prove elettroniche» (art. 2 (1)). L'"ordine di conservazione europeo" è, invece, un provvedimento «vincolante di un'autorità di emissione di uno Stato membro che ingiunge a un prestatore di servizi […] di conservare prove elettroniche in vista di una successiva richiesta di produzione» (art. 2 (2)). Degne di nota sono poi le definizioni delle singole tipologie di informazioni digitali che possono essere domandate tramite un OPE o un OCE[54], le quali sono suddivise in "*subscriber data*" (dati relativi agli abbonati), "*access data*" (dati relativi agli accessi), "*transactional data*" (dati relativi alle operazioni) e "*content data*" (dati relativi al contenuto).

---

[47] Cfr. *proposta di Regolamento*, cit., p. 12.

[48] Pare infatti utile precisare che «l'ordine europeo di produzione e l'ordine europeo di conservazione sono atti di indagine che possono essere emessi solo nell'ambito di un'indagine penale o di un procedimento penale per un reato concreto. Il nesso con un'indagine concreta distingue tali ordini dalle misure preventive e dagli obblighi di conservazione dei dati stabiliti dalla legge e garantisce l'applicazione dei diritti procedurali applicabili nei procedimenti penali». In questo senso si esprime la *proposta di Regolamento*, cit., p. 16.

[49] L'art. 3, par. 2 precisa, infatti, che «gli ordini possono essere emessi anche per procedimenti relativi a reati per i quali una persona giuridica può essere considerata responsabile o punibile nello Stato di emissione».

[50] Nel contesto della *proposta di Regolamento*, per prova elettronica si intende «le prove conservate 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, consistenti nei dati conservati relativi agli abbonati, agli accessi, alle operazioni o al contenuto» (così, art. 2 (6)).

[51] V. l'art. 2 (3) della *proposta di Regolamento*.

[52] Si vedano sul punto i considerando 26-28 della *proposta di Regolamento*.

[53] Cfr. considerando 17 e l'art. 1 della *proposta di Regolamento*.

[54] Cfr. art. 2 (7-10) e considerando 20-23 della *proposta di Regolamento*.

3.2. Capo II: autorità legittimate, condizioni di operatività e funzionamento delle misure.

Nel Capo II dell'atto (art. 4-12 e considerando 30-44)[55] è racchiuso il vero cuore operativo del sistema di circolazione probatoria ideato dalla Commissione.

L'art. 4 stabilisce le autorità nazionali competenti a emanare gli ordini europei in esame: quest'ultimi possono essere adottati unicamente da giudici, pubblici ministeri e, a determinate condizioni, anche da «qualsiasi altra autorità competente, definita dallo Stato di emissione che, nel caso di specie, agisca in qualità di autorità inquirente nel procedimento penale e sia competente a disporre l'acquisizione di prove in conformità del diritto nazionale»[56].

La Commissione ha attualmente previsto una disciplina eterogenea per gli ordini di produzione e conservazione europei, a seconda della tipologia di informazioni digitali di cui necessitino le autorità nazionali[57]. Difatti, soltanto gli OCE possono essere emessi autonomamente da un pubblico ministero, senza una previa validazione di un giudice, anche nel caso in cui abbiano a oggetto "dati relativi alle operazioni o al contenuto"[58]. Per converso, gli OPE, per tali tipologie di dati, devono quantomeno essere convalidati da un giudice. Dal canto loro, le "altre autorità competenti" necessitano sempre dell'autorizzazione di un magistrato, soggetto che deve essere per forza un giudice nel caso degli OPE disposti per ottenere "*transactional* e *content data*"[59].

I destinatari delle richieste sono, invece, stabiliti dall'art. 7 e dal considerando 37, i quali prevedono, come regola generale, che gli OPE e gli OCE vadano spediti ai rappresentanti legali, specificamente designati dai *service provider* al fine di ricevere richieste di prova nel corso di un procedimento penale, in ossequio a quanto previsto dalla proposta di Direttiva COM (2018) 226 final[60]. Nei successivi paragrafi della disposizione sono invece dettati criteri speciali, che operano qualora il fornitore di servizi non abbia (ancora) nominato il suddetto rappresentante, oppure in casi di particolare urgenza.

Gli artt. 5 e 6 precisano, invece, le condizioni di applicabilità, rispettivamente, degli ordini di produzione e di conservazione europei.

Anche in questo caso l'iniziativa legislativa prescrive per gli OPE (in ragione della loro maggiore afflittività) requisiti più stringenti di quelli stabiliti per gli OCE.

La proposta stabilisce infatti che gli OPE, aventi a oggetto "dati relativi alle operazioni o al contenuto", possono essere disposti soltanto nei procedimenti penali per alcune fattispecie di reato armonizzate dal legislatore europeo espressamente

---

[55] Cfr. *proposta di Regolamento*, cit., p. 12 s.

[56] Si vedano i par. 1 (b), 2 (b) e 3 (b) dell'art. 4 della *proposta di Regolamento*. In tale assai ampia categoria sembra rientrare, ad esempio, la polizia giudiziaria.

[57] Pare infatti utile chiarire che i dati relativi alle operazioni o al contenuto sono stati considerati più sensibili – e quindi bisognosi di maggiori tutele – rispetto a quelli concernenti l'accesso o l'abbonamento. Sul punto si vedano, esplicitamente, i considerando 30 e 31 della *proposta di Regolamento*.

[58] Cfr. art. 4, par. 1 e 2, nonché il considerando 30, della *proposta di Regolamento*.

[59] Si vedano i par. 1 (b) e 2 (b) dell'art. 4 della *proposta di Regolamento*.

[60] Cfr. *sub* § 4.

individuate (come il terrorismo, la pornografia minorile o gli abusi sessuali sui minori), oppure per i reati puniti nel massimo con almeno tre anni di pena detentiva (art. 5, par. 4).

Al contrario, gli OPE, concernenti dati relativi agli accessi o agli abbonati, possono essere emessi per qualsiasi illecito penale (art. 5, par. 3).

L'art. 5, par. 2, da leggersi assieme al considerando n. 33, precisa che tutti gli ordini di produzione europei (apparentemente anche se aventi a oggetto "*subscriber o* "*access data*") possono essere adottati «solo se una misura dello stesso tipo è disponibile per lo stesso reato in una situazione nazionale comparabile nello Stato di emissione». L'ultimo paragrafo di tale disposizione stabilisce poi una disciplina speciale, che opera nel caso in cui l'autorità nazionale di emissione di un OPE ritenga che i *transactional* o *content data* da richiedere siano protetti da "immunità" o "privilegi"[61], secondo il diritto nazionale dello Stato membro dove è allocato il *service provider*, oppure ove la *disclosure* degli stessi possa impattare su interessi fondamentali di detto Paese, come la difesa o la sicurezza nazionale[62].

Nessuna di queste regole è prevista per gli ordini di conservazione europei: quest'ultimi possono quindi essere adottati, indipendentemente dalla tipologia di dati in gioco, per ogni reato (art. 6, par. 2).

Esiste però una fondamentale condizione di applicabilità comune a entrambe le misure in esame: per essere emanati sia gli OPE, sia gli OCE devono sempre superare un *test* concreto, svolto da parte della singola autorità nazionale, di "proporzionalità" e "necessità" dell'atto[63]. L'iniziativa normativa non chiarisce, invece, allo stato in modo espresso alcuno *standard* probatorio da rispettare per poter adottare un OPE o un OCE[64].

È degno di nota il fatto che la proposta di Regolamento non utilizzi il concetto di "doppia incriminazione": essa richiede, infatti, soltanto che un'autorità nazionale proceda per un reato secondo il diritto penale di uno Stato membro. Come è stato giustamente osservato, «*this presumes a high level of confidence in the adherence to fundamental rights in all Member States*»[65].

Negli articoli da 8 a 10 viene descritto il funzionamento pratico delle misure in esame. In estrema sintesi, a circolare effettivamente è un certificato di ordine di produzione o di conservazione europeo[66] (i cui contenuti sono prestabiliti in una serie di modelli allegati alla proposta di Regolamento[67]), che viene prima completato con i dati concreti della singola regiudicanda dall'autorità di emissione o di validazione e poi

---

[61] A tale riguardo il considerando 35 della *proposta di Regolamento* pone l'esempio di dati concernenti diplomatici o quelli riguardanti il rapporto tra un legale e il proprio cliente.

[62] Si veda sul punto anche l'art. 18 della *proposta di Regolamento*.

[63] Si vedano i parr. 2 degli art. 5 e 6 della *proposta di Regolamento*.

[64] Cfr., a riguardo, J.-H. JEPPESEN – G. NOJEIM, *Assessing the European Commission's E-Evidence Proposals on Ten Human Rights Criteria*, in www.cdt.org, 18 aprile 2018, i quali precisano che «*issuing authorities are required to assess necessity and proportionality before issuing orders, and decisions of the European Court of Human Rights call for "reasonable suspicion" and even "probable cause," as part of such assessment*».

[65] In questo senso cfr. J.-H. JEPPESEN – G. NOJEIM, *Initial Observations*, cit.

[66] Art. 8 della *proposta di Regolamento*.

[67] Cfr. il *documento della Commissione europea* COM (2018) 225 final.

spedito direttamente al *service provider*. Ove necessario, i certificati vanno tradotti «in una lingua ufficiale dello Stato membro del destinatario o in un'altra lingua ufficiale che il prestatore di servizi abbia dichiarato di accettare» (considerando 38).

Una volta che un certificato contenente un OPE sia giunto al fornitore di servizi (*rectius* al suo legale rappresentante) questi è tenuto a spedire la prova informatica secondo delle rigide scansioni temporali stabilite dall'art. 9: ciò deve avvenire, in linea di principio, al più tardi entro dieci giorni da quando la misura è ricevuta, a meno che l'autorità emittente non indichi delle ragioni per cui è necessaria una "consegna" più rapida (art. 9, par. 1). Nei cosiddetti casi di emergenza di cui all'art. 9, par. 2, della proposta i dati richiesti vanno trasmessi senza ritardo e, al più tardi, entro 6 ore. I paragrafi successivi dell'art. 9 disciplinano poi le fattispecie in cui il *provider* abbia difficoltà a eseguire l'OPE, in ragione del fatto che esso contenga informazioni incomplete, errori manifesti o per cause di forza maggiore.

Per quanto concerne le modalità esecutive degli OCE viene, invece, in gioco l'art. 10, il quale precisa, tra l'altro, che, una volta ricevuto tale certificato, il *service provider* deve, senza indebito ritardo, preservare i dati richiesti. La conservazione dei dati cessa dopo 60 giorni, a meno che l'autorità richiedente confermi che è stata avviata una successiva richiesta di produzione.

Il principale valore aggiunto della proposta rispetto allo *status quo* sarà quindi oramai chiaro: ove effettivamente fosse messo a regime e funzionasse a dovere, lo strumento di cooperazione in esame consentirebbe di portare a termine la procedura di spedizione o di conservazione delle prove elettroniche in pochi giorni o ore. Al contrario, attualmente la Direttiva sull'OEI – la quale è già più rapida rispetto agli strumenti di mutua assistenza giudiziaria con Stati terzi – prevede tempi di consegna del materiale probatorio quantificabili in 120 giorni[68].

Come anticipato, varie disposizioni dell'atto hanno il fine di proteggere i diritti fondamentali degli indagati e imputati coinvolti nella procedura[69]: tra queste spiccano gli artt. 9, par. 5 e 14, par. 4 (f), i quali consentono ai *service provider* di opporsi alla consegna dei dati, quando appaia che un OPE violi la Carta dei diritti fondamentali dell'Unione europea o risulti manifestamente abusivo[70]. Si tratta, come è ovvio, di una

---

[68] In questo senso, espressamente, si esprime l'*Impact assessment*, p. 23.

[69] Il considerando 56 della *proposta di Regolamento* chiarisce, ad esempio, che gli Stati membri «dovrebbero assicurare che i dati personali siano protetti e possano essere trattati solo in conformità del regolamento (UE) 2016/679 e della direttiva (UE) 2016/680». Si vedano sul punto anche i considerando 13, 23, 43 e 57. Il considerando 14 precisa, invece, che il Regolamento sugli OPE e OCE deve essere applicato senza pregiudizio ai diritti processuali degli accusati, stabiliti nelle Direttive 2010/64/UE, 2012/13/UE, 2013/48/UE, 2016/343/UE, 2016/800/UE e 2016/1919/UE. Più in generale, l'art. 1, par. 2, della proposta statuisce che «il presente regolamento non ha l'effetto di modificare l'obbligo di rispettare i diritti fondamentali e i principi giuridici sanciti dall'articolo 6 TUE, compresi i diritti di difesa delle persone sottoposte a procedimento penale, e lascia impregiudicati gli obblighi spettanti a tale riguardo alle autorità di contrasto o giudiziarie».

[70] Per un esempio cfr. il considerando 55 della *proposta di Regolamento*, ove si precisa che «un ordine che chieda la produzione di dati relativi al contenuto riguardanti una categoria indeterminata di persone in un'area geografica, o che non ha alcun collegamento concreto con un procedimento penale, ignorerebbe in modo manifesto le condizioni per l'emissione dell'ordine europeo di produzione».

disposizione chiave, posto che è idonea a evitare che gli OPE si trasformino in una trappola lesiva dei più basilari principi dell'Unione, racchiusi nella Carta di Nizza.

Un particolare bilanciamento tra diritti fondamentali del prevenuto ed esigenze repressive della collettività è contenuto all'art. 11[71]: tale previsione vieta ai *service provider* di informare dell'OPE o dell'OCE i titolari dei dati, ove l'autorità giudiziaria emittente lo richieda per preservare l'efficienza delle indagini (art. 11, par. 1). In tale fattispecie saranno le autorità che hanno richiesto la misura, una volta che la prova elettronica sia stata loro consegnata, a dover informare "senza ritardo" gli interessati[72], potendo però posticipare questo adempimento «per il tempo necessario e proporzionato per non ostacolare il pertinente procedimento penale» (art. 11, par. 2).

Va in ultima analisi ricordato che l'art. 12 della proposta stabilisce che i fornitori di servizi potranno chiedere allo Stato d'origine dell'autorità richiedente il rimborso dei costi sostenuti nel corso della procedura di consegna o di conservazione delle prove elettroniche, se ciò è stabilito dal diritto nazionale per delle misure investigative corrispondenti.

3.3. Le restanti disposizioni della proposta di Regolamento: sanzioni, rimedi e previsioni finali.

Il Capo III della proposta (articoli 13 e 14 e considerando 44-45 e 55)[73] ha lo scopo di assicurare l'effettività del sistema di circolazione probatoria diretta ideato dalla Commissione europea. Difatti, onde assicurarsi che le norme UE siano prese sul serio, l'art. 13 impone anzitutto agli Stati di stabilire sanzioni pecuniarie (effettive, dissuasive e proporzionate) nei confronti dei soggetti che violino gli obblighi derivanti dagli artt. 9, 10 e 11.

L'art. 14 prevede, invece, una complessa procedura esecutiva avverso i *providers* inadempimenti alle richieste di prove elettroniche transnazionali. In tali fattispecie ritornano in campo le autorità giudiziarie dello Stato di esecuzione, le quali sono tenute a riconoscere l'OPE o l'OCE e a obbligare il detentore del dato a produrlo all'autorità richiedente o a conservarlo, salvo in determinate fattispecie stabilite in via tassativa nella proposta (art. 14, parr. 2, 4 e 5, ove è racchiusa una serie tassativa di motivi di opposizione ammissibili nei confronti delle misure europee)[74].

Il Capo IV (artt. 15-18, da leggere insieme ai considerando 35 e da 47-54)[75] detta poi un'eterogenea disciplina in materia di rimedi.

Gli articoli 15 e 16 vanno letti congiuntamente: essi stabiliscono due procedure speciali per i casi in cui il destinatario di un OPE (e non di un OCE) ritenga che

---

[71] Si tratta di una disposizione ispirata dall'art. 19 della Direttiva 2014/41/UE.

[72] La Commissione ha sul punto chiarito che «a causa del minore impatto sui diritti coinvolti, tali informazioni sono fornite solo per l'ordine europeo di produzione, non per l'ordine europeo di conservazione». Cfr., in questo senso, la *proposta di Regolamento*, cit., p. 21.

[73] Cfr. *proposta di Regolamento*, cit., p. 12.

[74] Si veda anche l'allegato III, contenuto nel *documento della Commissione* COM (2018) 225 final.

[75] Cfr. *proposta di Regolamento*, cit., p. 12.

l'ottemperanza a tale misura europea si ponga in contrasto con il diritto applicabile di uno Stato terzo, che vieti la divulgazione dei dati richiesti per diversi ordini di ragioni (tra cui la protezione dei diritti fondamentali dell'individuo, oppure per motivi di sicurezza o difesa nazionale). In tale fattispecie, in buona sostanza, il *provider* si troverebbe di fronte a «obblighi contrastanti»: gli uni derivanti dal Regolamento UE e gli altri dal diritto del Paese terzo. Per risolvere questa *impasse* la proposta prevede – tra l'altro – un possibile coinvolgimento di un'autorità giudiziaria dello Stato di emissione e, nel caso sia in gioco un contrasto tra OPE e diritti fondamentali dell'individuo, oppure ragioni di sicurezza o difesa nazionale dello Stato terzo, eventualmente, anche delle autorità centrali di tale Paese[76], individuate tramite i canali di mutua assistenza giudiziaria. Si tratta, come ovvio, di norme che assumono un particolare rilievo nell'economia complessiva dell'atto, posto che molti *service provider* chiave hanno il quartier generale fuori dallo SLSG (si pensi soltanto a Facebook o Google). È importante notare come la Commissione, avendo fissato in tali disposizioni un elevato *standard* di garanzie, abbia perseguito lo scopo di instaurare un circolo virtuoso, incoraggiando «i paesi terzi a prevedere un livello di tutela analogo»[77].

Dal canto suo, l'art. 17 della proposta assicura, nuovamente ai soli individui destinatari di un ordine di produzione europeo (e non di un OCE)[78], un «*effective remedy*», esperibile dinnanzi a un giudice nazionale dello Stato di emissione della misura. Questa previsione conferma la recente prassi dell'Unione di inserire nei suoi atti di diritto derivato norme riproduttive dell'art. 47, par. 1, della Carta dei diritti fondamentali dell'Unione[79]. Il rimedio europeo di cui all'art. 17 della proposta dovrà consentire di contrastare la legalità dell'OPE, inclusa la sua necessità e proporzionalità (art. 17, par. 3).

L'art. 17, par. 6, dell'atto chiarisce poi che gli Stati membri devono assicurare che «nei procedimenti penali nello Stato di emissione siano rispettati i diritti della difesa e sia garantito un giusto processo nel valutare le prove acquisite tramite l'ordine europeo di produzione». Si tratta di una disposizione sostanzialmente gemella a quelle contenute negli art. 12, par. 2 e 10, par. 2, rispettivamente, della Direttiva 2013/48/UE e 2016/343/UE[80], che va però letta assieme al considerando 54 della proposta, ove si stabilisce – tra l'altro – che l'esercizio del rimedio effettivo *de quo* da parte dell'indagato o imputato «può incidere sull'ammissibilità delle prove ottenute con detti mezzi o, a seconda del caso, sul peso di tali prove nell'ambito del procedimento». La Commissione sembra aver così tentato di adottare una previsione più coraggiosa in tema di rimedi

---

[76] Si veda i considerando 49, 51 e l'art. 15, par. 5, della *proposta di Regolamento*.

[77] Cfr. *proposta di Regolamento*, cit., p. 22.

[78] Si veda sul punto la *proposta di Regolamento*, cit., p. 23, dove si ammette espressamente che «il diritto a un ricorso effettivo non è disponibile per l'ordine europeo di conservazione, giacché tale ordine di per sé non consente la divulgazione dei dati; tuttavia qualora esso sia seguito da un ordine europeo di produzione o da un altro strumento che comporta la divulgazione dei dati il ricorso è possibile in virtù di questi strumenti».

[79] Ciò è, ad esempio, avvenuto nelle Direttive 2013/48/UE, 2016/343/UE, 2016/800/UE e 2016/1919/UE.

[80] Sulle quali si consenta il rinvio a J. DELLA TORRE, *Le direttive UE sui diritti fondamentali degli accusati: pregi e difetti del primo "embrione" di un sistema europeo di garanzie difensive*, in *Cass. pen.*, 2018, p. 1413 s.

rispetto a quelle contenute nelle Direttive di Stoccolma[81]: nel considerando della proposta di Regolamento in esame si ammette infatti finalmente in modo espresso che la violazione delle norme europee può andare a incidere sul piano dell'ammissibilità[82] o della valutazione del materiale probatorio raccolto. Sarà interessante verificare se nel corso delle future negoziazioni il Consiglio UE chiederà di eliminare tale disposizione dall'iniziativa normativa, come, ad esempio, ha già fatto e ottenuto in passato, quando il Parlamento europeo e la Commissione avevano tentato di inserire nella Direttiva 2016/343/UE delle regole di esclusione (rispettivamente secche o discrezionali) per "sanzionare" la violazione del diritto al silenzio e di non collaborare[83].

La proposta si chiude con una nutrita serie di previsioni finali (Capo V – art. 19-25, considerando 58-62)[84], tra cui spicca l'art. 23, il quale è vòlto a regolare i rapporti tra il Regolamento in materia di circolazione delle prove elettroniche e l'OEI. Mediante tale disposizione la Commissione ha voluto precisare che, anche nel caso in cui fosse effettivamente approvata la proposta in commento, gli Stati membri potranno comunque continuare a utilizzare la Direttiva 2014/41/UE per richiedere prove elettroniche, il che potrebbe, ad esempio, avere un senso quando l'autorità di emissione necessiti di ricevere da un altro Stato diversi elementi istruttori, di cui solo alcuni informatici[85], e non via sia il timore che i dati elettronici vengano alterati o dispersi.

---

[81] In merito alla tematica dei rimedi nelle Direttive volte a rafforzare i diritti processuali degli indagati e imputati, si vedano, tra i molti, M. CAIANIELLO, *Procedural Sanctions in the Eu Framework: Toward a Harmless Error Doctrine and Practice*?, in *Discretionary Criminal Justice in a Comparative Context*, a cura di M. Caianiello e J. Hodgson, Durham, 2015, p. 207 ss.; ID., *To Sanction (or not to Sanction) Procedural Flaws at EU Level?*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2014, p. 317 ss.; O. MAZZA, *Presunzione d'innocenza e diritto di difesa*, in *Dir. pen. proc.*, 2014, p. 1409; A. SOO, *Article 12 of the Directive 2013/48/EU: A Starting Point for Discussion on a Common Understanding of the Criteria for Effective Remedies of Violation of the Right to Counsel*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2017, p. 32 ss.; EAD., *(Effective) Remedies for a Violation of the Right to Counsel during Criminal Proceedings in the European Union: An Empirical Study*, in *Utrecht Law Review*, 2018, p. 18 ss.; EAD., *Potential Remedies for Violation of the Right to Counsel in Criminal Proceedings: Article 12 of the Directive 2013/48/EU (22 October 2013) and its Output in National Legislation*, in *European Criminal Law Review*, 2016, p. 284 ss.

[82] Si veda anche l'art. 18 della *proposta di Regolamento*, il quale stabilisce espressamente che «se i dati relativi alle operazioni o al contenuto ottenuti tramite l'ordine europeo di produzione sono protetti con immunità o privilegi ai sensi del diritto dello Stato membro del destinatario, o incidono su interessi fondamentali di tale Stato membro come la sicurezza e la difesa nazionali, l'organo giurisdizionale dello Stato di emissione garantisce, durante il procedimento penale per il quale l'ordine è stato emesso, che nel valutare la pertinenza e l'ammissibilità delle prove in questione tali motivi siano presi in considerazione come se fossero previsti dal suo diritto nazionale».

[83] Cfr. J. DELLA TORRE, *Il paradosso della direttiva sul rafforzamento della presunzione di innocenza e del diritto di presenziare al processo: un passo indietro rispetto alle garanzie convenzionali?*, in *Riv. it. dir. proc. pen.*, 2016, p. 1873 s.

[84] V. *proposta di Regolamento*, cit., p. 13.

[85] In questo senso si esprime il considerando 61 della *proposta di Regolamento*.

4. La proposta di Direttiva sulla nomina dei rappresentati legali per finalità legate alla raccolta delle prove nei procedimenti penali.

Come anticipato, il pacchetto di intervento presentato dalla Commissione europea è completato da una proposta di Direttiva, «recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali».

Anche tale seconda iniziativa – fondata sugli articoli 53 e 62 TFUE[86] – mira a risolvere la situazione di incertezza e frammentazione normativa in cui attualmente operano i *service provider* e le autorità nazionali, la quale non impedisce soltanto di perseguire una grande quantità di reati nello SLSG, ma – secondo la Commissione – è idonea a creare anche un ostacolo al principio fondamentale della libera prestazione dei servizi[87].

L'intera proposta di Direttiva ruota attorno all'obbligo, posto in capo agli Stati membri, di provvedere affinché alcune categorie di *providers*[88] – che offrono servizi nell'UE [89], pure nel caso in cui abbiano la sede centrale in un Paese terzo[90] – nominino almeno un rappresentante legale, competente per la ricezione, il rispetto e l'esecuzione delle decisioni e degli ordini emessi dalle autorità nazionali ai fini dell'acquisizione di prove penali[91].

Pare utile precisare che allo stato attuale delle negoziazioni tale rappresentante legale:

a) potrebbe essere una persona fisica o giuridica (art. 2 (2));

b) dovrebbe risiedere in uno Stato membro dove il *service provider* sia stabilito o fornisca le sue prestazioni (art. 3, par. 1 e 2);

c) non avrebbe il compito di ricevere soltanto un OCE o un OPE, ma ogni richiesta probatoria proveniente da un'autorità penale di uno Stato membro[92];

---

[86] Cfr. *proposta di Direttiva*, cit., p. 4.

[87] Cfr. i considerando 3 e 5 della *proposta di Direttiva*.

[88] Si veda l'art. 2 (2) della *proposta di Direttiva*.

[89] Cfr. art. 1, par. 4, ove si precisa che la Direttiva «non si applica ai prestatori di servizi stabiliti sul territorio di un singolo Stato membro che offrono servizi esclusivamente sul territorio di tale Stato membro».

[90] Cfr. art. 3, par. 2, della *proposta di Direttiva*.

[91] Come precisa l'art. 3, par. 4, della *proposta di Direttiva*, «i prestatori di servizi sono liberi di designare rappresentanti legali aggiuntivi che risiedono o sono stabiliti in altri Stati membri, compresi quelli in cui i prestatori di servizi offrono i servizi. I prestatori di servizi che fanno parte di un gruppo sono autorizzati a designare collettivamente un solo rappresentante legale».

[92] Si veda, in particolare, sul punto il considerando 8 della *proposta di Direttiva*, ove si stabilisce che «il rappresentante legale in questione dovrebbe fungere da destinatario di ordini e decisioni nazionali e di ordini e decisioni emessi in conformità degli strumenti giuridici dell'Unione adottati a norma del titolo V, capo 4, del trattato sul funzionamento dell'Unione europea per acquisire prove in materia penale». Pare utile ricordare che il considerando 14 di tale iniziativa precisa, oltretutto, che «la designazione di un rappresentante legale, che potrebbe servire anche a garantire l'ottemperanza agli obblighi giuridici nazionali, permetterebbe di trarre vantaggio dalle sinergie derivanti dalla presenza di un chiaro punto di accesso unico per rivolgersi ai prestatori di servizi al fine di acquisire prove in materia penale».

d) dovrebbe essere dotato di poteri e risorse idonee per ottemperare effettivamente le decisioni o gli ordini nazionali[93].

La Commissione ha poi ideato un secondo meccanismo complementare alla nomina dei rappresentati legali: l'art. 6[94] mira infatti a obbligare gli Stati a creare una o più autorità centrali, a cui verrebbero affidati alcuni compiti specifici, tra cui quello di cooperare reciprocamente, oppure con la Commissione, «per applicare la presente direttiva in modo coerente e proporzionato» (art. 6, par. 4).

Gli effetti positivi che avrebbe l'approvazione di tale iniziativa normativa sono chiari[95]. La nomina di uno o più rappresentati legali nell'Unione, deputati alla circolazione delle prove penali, porterebbe, da un lato, i *service providers* a dotarsi finalmente di un apparato organizzativo adeguato a soddisfare le frequenti richieste probatorie degli Stati membri e, da un altro lato, le autorità nazionali a sapere con precisione come e a chi rivolgersi per ottenere il materiale probatorio di cui necessitano[96].

5. Riflessioni di sintesi.

La presentazione da parte della Commissione europea delle due iniziative qui pubblicate non può che essere salutata con favore. Tramite tale pacchetto di intervento l'Unione ha dimostrato di essere ben conscia del fatto che la circolazione delle prove elettroniche rappresenti una delle maggiori sfide della modernità, che possono minare alla radice il proposito di costruire un effettivo spazio di libertà, sicurezza e giustizia comune. In tal modo la "piccola Europa" ha oltretutto dato una precisa riprova di voler stare al passo, non solo con gli Stati Uniti, che nei primi mesi del 2018 hanno approvato un'importante riforma concernente proprio la circolazione transnazionale delle prove digitali[97], ma soprattutto con il Consiglio d'Europa. È infatti noto che, a sua volta, tale organizzazione internazionale ha avviato i negoziati per la stipula di un secondo protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica, finalizzato a rimediare alle numerose lacune, ben poste in rilievo dal *Cybercrime Convention Committee*, a cui è andato incontro il fondamentale trattato internazionale *de quo*[98]. Si badi: l'effettiva creazione di tale protocollo sarebbe un fatto di primaria

---

[93] Art. 3, par. 7 e considerando 18 della *proposta di Direttiva*.

[94] Tale previsione va letta assieme al considerando 22 della proposta.

[95] Si veda, a riguardo, la *proposta di Direttiva*, cit., p. 4.

[96] Cfr. l'art. 4 della *proposta di Direttiva*, il quale stabilisce che «gli Stati membri provvedono affinché ogni prestatore di servizi che è stabilito od offre servizi nel loro territorio, dopo aver designato il proprio rappresentante legale in conformità dell'articolo 3, paragrafi 1, 2 e 3, notifichi per iscritto la designazione e i dati di contatto del rappresentante legale, nonché loro eventuali modifiche, all'autorità centrale dello Stato membro in cui il rappresentante legale risiede o è stabilito».

[97] Ci si riferisce al *Clarifying Lawful Overseas Use of Data ("CLOUD") Act*, del 23 marzo 2018. Per un commento, cfr. J. GARLAND – A. BERENGAUT – K. GOODLOE, *CLOUD Act Creates New Framework for Cross-Border Data Access*, in www.insideprivacy.com, 26 marzo 2018.

[98] Si veda, ad esempio, il documento *T-CY (2017) 3*, (*DRAFT) Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime*, disponibile a questo *link*.

importanza per i Paesi europei; e ciò in quanto anche Stati chiave nella circolazione mondiale delle prove elettroniche (tra cui proprio gli USA) fanno parte della Convenzione di Budapest e potrebbero quindi firmare e ratificare il nuovo atto (a cui sarebbe assai auspicabile partecipasse direttamente anche l'Unione[99]).

Per quanto concerne il metodo seguito, pare degno di nota il fatto che la Commissione abbia deciso di presentare una proposta di Regolamento al fine di istituire gli OPE e OCE, non utilizzando lo strumento della Direttiva, come aveva invece fatto nel 2014 per l'OEI, che pur era fondato sulla stessa base giuridica dell'art. 82, par. 1, TFUE. Tale scelta è stata così giustificata: «poiché la proposta riguarda procedure transfrontaliere, per le quali sono necessarie norme uniformi, non occorre lasciare un margine agli Stati membri per recepirle. Il regolamento è direttamente applicabile, offre chiarezza e maggiore certezza giuridica e consente di evitare interpretazioni divergenti negli Stati membri e altri problemi di recepimento incontrati dalle decisioni quadro sul riconoscimento reciproco delle sentenze e delle decisioni giudiziarie»[100]. Tutto ciò fornisce una precisa riprova di quanto l'Unione oramai si fidi talmente poco di come gli Stati membri sono soliti recepire gli atti eurounitari in materia processuale penale, da aver tentato in questo caso di bypassare alla radice ogni problema di attuazione interna, proponendo un atto *self-executing*.

Da un punto di vista contenutistico, le proposte in esame presentano diversi difetti (anche piuttosto gravi): nei due testi – caratterizzati da una prosa assai difficile e tecnica – vi sono, infatti, numerosi punti oscuri e lacune.

Peraltro, l'aspetto più delicato, che riguarda soprattutto la proposta di Regolamento, concerne l'apparato delle tutele predisposte nei confronti dei soggetti coinvolti nella procedura. Sembra, infatti, che il proposito della Commissione di creare un meccanismo di circolazione delle prove elettroniche fortemente garantista non sia stato – al di là dei proclami – effettivamente rispettato. Al contrario, l'iniziativa ha previsto in diversi casi diritti solo minimali, di modo che il testo necessiterebbe un sensibile innalzamento delle garanzie nel corso delle negoziazioni[101].

A tal proposito, sembrano essere sufficienti due esempi.

In primo luogo, va notato che la Commissione ha prestato la maggior parte delle sue attenzioni nei confronti dell'OPE (specie se concernente dati relativi alle operazioni o al contenuto), mentre ha tralasciato gli ordini di conservazione europei. Così facendo, ha dato vita per questi ultimi a un regime assai sbilanciato in favore delle esigenze repressive rispetto a quelle di tutela dei diritti fondamentali. Del resto, se è pur vero che

---

[99] Pare utile precisare che tra le priorità dell'UE relative alla cooperazione con il Consiglio d'Europa per il periodo 2018/2019, adottate dal Consiglio UE il 22 gennaio 2018, vi è proprio quella di «proseguire la cooperazione nel quadro della Convenzione di Budapest sulla criminalità informatica e dei suoi protocolli addizionali; garantire la coerenza tra il secondo protocollo addizionale in corso di negoziazione e i lavori dell'UE relativi al miglioramento dell'accesso transfrontaliero alle prove elettroniche; promuovere la Convenzione di Budapest quale quadro per la cooperazione internazionale e lo sviluppo di capacità». In questo senso si esprime il *documento del Consiglio UE, 5553/18*, p. 9.

[100] Cfr. *proposta di Regolamento*, cit., p. 6.

[101] In questo senso si esprimono anche J.-H. JEPPESEN – G. NOJEIM, *Assessing the European Commission's E-Evidence Proposals*, cit.

la consegna dei dati informatici a un'autorità a fini penalistici incide in modo più gravoso sui diritti di un individuo rispetto al mero obbligo di conservarli inalterati, il fatto stesso che un individuo, per un certo periodo di tempo, non possa avere la libera disponibilità di informazioni che lo riguardano è comunque una forma di intrusione nella sua sfera di libertà, che pare necessitare di tutele più intense rispetto a quelle stabilite nella proposta in commento. A tale riguardo, basti pensare al fatto che, come accennato, la Commissione non ha neppure previsto che i destinatari di un OCE abbiano diritto a un *effective remedy* per contestare l'illegalità della misura[102]. Questa scelta di politica normativa non pare affatto condivisibile, posto che sembra porsi in contrasto con l'art. 47, par. 1, della CDFUE. Tale disposizione della Carta di Nizza assicura, infatti, a ogni individuo che veda lesi i suoi diritti attribuiti dall'Unione – e quindi di certo anche a coloro nei cui confronti sia stato emanato un OCE – il diritto a un mezzo di ricorso effettivo[103]. È di conseguenza auspicabile che, nell'incedere dei lavori preparatori, le istituzioni UE ritornino sui loro passi e garantiscano espressamente la possibilità di esperire un "*effective remedy*" anche per gli ordini di conservazione europei.

Un secondo esempio, che testimonia l'atteggiamento securitario tenuto dalla Commissione, pare poter essere individuato nelle (assai ampie) condizioni di applicabilità che la proposta ha stabilito per emanare gli OPE e gli OCE. Dato il valore fondamentale dei diritti degli indagati e imputati in gioco nella procedura in esame, non sembra, infatti, condivisibile la scelta di consentire alle autorità nazionali – salvo che per gli OPE concernenti *transnactional* e *content data* – di utilizzare tali mezzi di ricerca della prova informatici per ogni tipologia di reato, senza alcun limite edittale di sorta stabilito *ex ante*: il rischio infatti è che vi sia un abuso da parte delle autorità di *law enforcement* di strumenti investigativi potenzialmente assai invasivi[104]. Tale pericolo è vieppiù incrementato dalla scelta, parimenti criticabile, di non stabilire in modo espresso alcuno *standard* probatorio minimo di cui le autorità nazionali debbano verificare la sussistenza prima di attivare le misure in questione. I soli parametri della "necessarietà e proporzionalità" rischiano, insomma, di essere troppo vaghi per riuscire a costituire un argine sufficiente per proteggere i diritti fondamentali degli accusati[105].

Ad ogni modo, non rimane ora che attendere come si svilupperanno nei prossimi mesi le negoziazioni all'interno del Parlamento e del Consiglio e, in seguito, quelle interistituzionali. L'esperienza di quanto recentemente avvenuto per le Direttive di Stoccolma – in cui nel corso dei lavori preparatori il Consiglio UE ha sempre richiesto e ottenuto un deciso abbassamento del livello di tutela rispetto alle proposte della

---

[102] Cfr. *proposta di Regolamento*, cit., p. 22.

[103] Ciò sembra, del resto, essere ammesso anche dal considerando 54 della *proposta di Regolamento*, ove – almeno dal punto di vista letterale – si stabilisce che «è essenziale che tutte le persone i cui dati sono richiesti nel corso di indagini o procedimenti penali abbiano accesso a un ricorso giurisdizionale effettivo, in linea con l'articolo 47 della Carta dei diritti fondamentali dell'Unione europea».

[104] Secondo J.-H. JEPPESEN – G. NOJEIM, *Initial Observations*, cit., il fatto che gli ordini di produzione europei possano essere richiesti anche per reati particolarmente lievi «*creates a risk that providers will be inundated with such demands*».

[105] Cfr. sul punto anche J.-H. JEPPESEN – G. NOJEIM, *Assessing the European Commission's E-Evidence Proposals*, cit.

Commissione[106] – non fa ben sperare per un futuro innalzamento delle garanzie. L'emergenza terroristica che aleggia nell'Unione potrebbe infatti portare il legislatore UE ad accentuare ancor di più gli aspetti securitari del testo, senza prestare debita attenzione alla tematica delle garanzie. Insomma, la tentazione di approvare quanto più velocemente possibile un atto, anche a discapito del livello dei diritti proclamati in favore degli indagati e accusati, potrebbe essere forte: ed è proprio qui che l'Unione dovrà dar prova di maturità, dimostrando di voler realmente creare uno spazio comune basato non solo sul paradigma della sicurezza, ma anche (e forse soprattutto) su quello della libertà e della giustizia.

[106] Si veda, al riguardo, M. GIALUZ, *L'assistenza linguistica nel processo penale. Un meta-diritto fondamentale tra paradigma europeo e prassi Italiana*, Padova, 2018, p. 113.