IL NUOVO MONDO DELLA COOPERAZIONE GIUDIZIARIA IN MATERIA PENALE NELL'UNIONE EUROPEA: LE PROPOSTE DELLA COMMISSIONE EUROPEA SUGLI ORDINI DI PRODUZIONE E CONSERVAZIONE DI PROVE ELETTRONICHE (*E-EVIDENCE*)

di Alessandro Rosanò
(*assegnista di ricerca nell'Università di Torino*)

1. Nel racconto *La notte che bruciammo Chrome* e nel romanzo *Neuromante*, pubblicati rispettivamente nel 1982 e nel 1984, William Gibson utilizzò per la prima volta il termine cyberspazio. Nel romanzo, questo (all'epoca) nuovo concetto veniva descritto così: "Un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione, da bambini a cui vengono insegnati i concetti matematici… Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità. Linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci di una città, che si allontanano".

Negli anni Ottanta, tutto ciò poteva apparire come il frutto della fervida immaginazione di uno scrittore. A distanza di più di tre decenni, può ritenersi che quelle parole siano state quanto mai profetiche. La comunicazione ha assunto nuove forme, rapide e dematerializzate, grazie a strumenti quali le *e-mail* e le *app* (tra le altre, WhatsApp e Telegram). L'archiviazione, l'elaborazione e la trasmissione di informazioni è basata sempre di più sul ricorso al *cloud computing*. La condivisione di dati avviene a ritmi vertiginosi attraverso piattaforme sociali quali Facebook, Instagram e TikTok.

I fenomeni ora riassunti non sono estranei al mondo del diritto, le cui diverse branche provano a fare i conti con specifiche declinazioni di essi. Valgano per tutti i casi del diritto internazionale che si confronta con la nuova realtà della guerra cibernetica[1], del diritto penale

[1] Per un'introduzione, quanto alla letteratura italiana, G. Tappero Merlo, *Il dominio degli spazi: il cosmo, la cyberwar e l'urgenza di una dottrina operativa per la guerra futura*, in *La Comunità Internazionale* 2010, 535 ss. e G. Suffia, *Geografia delle cyberwars. Uomini e Stati alla prova dello spazio digitale*, Milano 2018; quanto alla letteratura di lingua inglese, J.P. Jurich, *Cyberwar and Customary International Law: The Potential of a "Bottom-up" Approach to an International Law of Information Operations*, in *Chicago Journal of International Law* 2008, 275 ss., K.E. Eichensehr, *Cyberwar & International Law Step Zero*, in *Texas International*

che fa i conti con l'emersione dei reati informatici[2] e del diritto processuale penale che assiste a una progressiva smaterializzazione delle prove[3].

Quest'ultima situazione, in particolar modo, assume rilievo non solo con riferimento ai reati informatici ma, ormai sempre di più, anche per quel che riguarda i reati comuni. Si pensi per esempio al fatto di poter stabilire se un determinato soggetto si trovava in un certo luogo a una certa ora attraverso la localizzazione del suo cellulare.

Si comprende allora l'interesse che le autorità giudiziarie e di polizia possono avere quanto all'accesso alle prove elettroniche (o *e-evidence*) e, soprattutto, quanto al fatto di accedervi nella maniera più rapida possibile. Si tratta infatti di realtà estremamente volatili. La formattazione del disco fisso di un computer o la cancellazione e sovrascrittura dei file salvati in una memoria usb possono compromettere l'integrità di alcuni dati e dunque le attività di indagine. A ciò deve necessariamente aggiungersi una conseguenza del *cloud-computing* che è il *data sharding*, ossia la conservazione di diverse parti di un database in server che sono dislocati in luoghi differenti nello stesso Stato o in Stati differenti[4].

Scopo del presente contributo è allora, una volta offerta una panoramica sul problema posto dalla ricerca delle prove elettroniche, illustrare il contenuto di due proposte formulate in materia da parte della Commissione europea e, una volta evidenziate le criticità fino ad ora riscontrate da parte di istituzioni e organi dell'Unione, *stakeholder* e dottrina, esprimere una ragione di critica ulteriore che emerge dalla lettura della proposta di regolamento e che riguarda la tecnica normativa utilizzata[5].

Law Journal 2015, 357 ss. e B.M. Mazanec, *The Evolution of Cyber War. International Norms for Emerging-Technology Weapons*, Lincoln 2015.

[2] Per un'introduzione, quanto alla letteratura italiana: L. Picotti (a cura), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova 2005; C. Pecorella, *Diritto penale dell'informatica*, Padova 2006; G. D'Aiuto, L. Levita, *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano 2012; A.C. Amato Mangiameli, G. Saraceni, *I reati informatici. Elementi di teoria generale e principali figure criminose*, Torino 2019 e A. Cadoppi, S. Canestrari, A. Manna, M. Papa, (diretto da), *Trattato di Diritto penale – Cybercrime*, Torino 2019. Quanto alla letteratura di lingua inglese: J. Clough, *Principles of Cybercrime*[2], Cambridge 2015; T.J. Holt, A.M. Bossler, *Cybercrime in Progress. Theory and prevention of technology-enabled offenses*, London-New York 2016 e R.S. Graham, S.K. Smith, *Cybercrime and Digital Deviance*, London-New York 2019.

[3] Per un'introduzione, quanto alla letteratura italiana, L. Luparia, G. Ziccardi (a cura di), *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano 2007; M. Daniele, *La prova digitale nel processo penale*, in *RDP* 2011, 294 ss., G. Vaciago, *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Torino 2012 e M.A. Biasiotti, *Presente e futuro dello scambio della prova elettronica in Europa*, in *Informatica e diritto* 2015, 35; quanto alla letteratura di lingua inglese, O.S. Kerr, *Digital Evidence and the New Criminal Procedure*, in *Columbia Law Review* 2005, 279 ss., E. Casey, *Digital Evidence and Computer Crime. Forensics Science, Computers and the Internet*[3], Waltham-San Diego-Londra 2011 e T.K. Clancy, *Cyber Crime and Digital Evidence. Materials and Cases*[3], Durham 2018.

[4] Al riguardo, P. Ryan, S. Falvey, *Trust in the Clouds*, in *Computer Law & Security Review* 2012, 28 ss. e P. M. Schwartz, *Legal Access to the Global Cloud*, in *Columbia Law Review* 2018, 1681 ss.

[5] Non è il tema del presente scritto, ma si sottolinea comunque che rimane aperta la questione dell'accesso a prove elettroniche che siano conservate al di fuori dell'Unione europea, la quale al momento può essere

2. Alla luce di quanto detto *supra*, può parlarsi di una progressiva digitalizzazione delle informazioni. Questo si ricollega all'attività svolta da parte di soggetti di diritto privato – prestatori di servizi telematici – i quali gestiscono e controllano quelle informazioni. L'interesse delle autorità investigative si rivolge sempre di più nei confronti di tali soggetti ma, posto che in molti casi essi non hanno sede nello Stato del cui potere sono espressione quelle autorità, emerge allora un fenomeno di deterritorializzazione[6], da cui deriva la forte esigenza di un'internazionalizzazione delle attività di indagine[7].

Al momento, nulla obbliga i prestatori di servizi telematici ad avere necessariamente una sede negli Stati in cui operino. Dunque, il problema che è emerso attiene alla possibilità di accedere a dati che siano conservati all'estero, ossia al di fuori della giurisdizione del singolo Stato interessato a ottenere certe prove elettroniche[8].

Al riguardo, deve darsi atto dell'apporto fornito dal diritto internazionale attraverso strumenti già esistenti e strumenti creati *ad hoc*. Quanto ai primi, può farsi riferimento alla Convenzione europea di assistenza giudiziaria in materia penale, conclusa nell'ambito del Consiglio d'Europa del 1959, la quale prevede forme di cooperazione fondate sull'emissione di rogatorie[9]. Quanto ai secondi, va menzionata la Convenzione sulla criminalità informatica del 2001, conclusa anch'essa nell'ambito del Consiglio d'Europa[10]. Diverse delle previsioni contenute in quest'ultima assumono rilievo ai fini della ricerca e dell'acquisizione di prove elettroniche, sia nel territorio nazionale (articoli 16-21), sia all'estero (articoli 29-34).

---

affrontata e risolta solo attraverso la conclusione di accordi internazionali. Per un'introduzione, V. Mitsilegas, *The New EU-US Co-operation on Extradition, Mutual Legal Assistance and the Exchange of Police Data*, in *European Foreign Affairs Review* 2003, 515 ss., J. Daskal, P. Swire, *A Possible EU-US Agreement on Law Enforcement Access to Data?*, in *Lawfare* 21.05.2018 e M. Plachta, *Second Round of Negotiations of an EU-U.S. Treaty on Access to Electronic Evidence*, in *International Enforcement Law Reporter* 2019, 453 ss. Per quel che riguarda i rapporti tra Unione europea e Stati Uniti, si segnala in particolar modo la proposta avanzata in S. Carrera, G. González Fuster, E. Guild, V. Mitsilegas, *Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights*, Brussels 2015, 79-80 quanto alla creazione di un ordine di indagine transatlantico fondato sulla fiducia reciproca intercorrente tra gli Stati membri dell'Unione e gli Stati Uniti (su quest'ultimo aspetto, E. Fahey, D. Curtin (eds), *A Transatlantic Community of Law. Legal Perspectives on the Relationship Between the EU and US Legal Orders*, Cambridge 2014).

[6] Per un'introduzione, D.R. Johnson, D.B. Post, *Law and Borders: The Rise of Law in Cyberspace*, in *Stanford Law Review* 1996, 1376 ss., M. Hildebrandt, *Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace*, in *University of Toronto Law Journal* 2013, 196 ss. e Ead., *The Virtuality of Territorial Borders*, in *Utrecht Law Review* 2017, 13 ss.

[7] Quanto a digitalizzazione delle prove, ruolo dei privati e internazionalizzazione delle attività di indagine, J. Daskal, *Unpacking the CLOUD Act*, in *Eucrim* 2018, 221

[8] R. Pezzuto, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, in *Diritto penale contemporaneo*, 1/2019, 59.

[9] Sulle rogatorie, G. Daraio, *Le rogatorie*, in G. Spangher (a cura di), *Procedura penale. Teoria e pratica del processo*, Milano 2015, 1065 ss.

[10] Per un'introduzione, R. Mazza, *Recenti sviluppi nella repressione internazionale dei crimini informatici: la*

Tanto con riferimento agli uni, quanto con riferimento agli altri strumenti, deve darsi atto di come essi non abbiano condotto a risultati significativi. In entrambi i casi, infatti, non sussiste un obbligo di cooperazione gravante in capo alle autorità dello Stato richiesto e comunque l'acquisizione delle prove avviene secondo la disciplina di tale Stato, con la conseguenza che dovranno rispettarsi i tempi e le procedure previsti a livello nazionale.

Ciò ha portato allo sviluppo in via di prassi di soluzioni fondate sulla richiesta diretta da parte delle autorità giudiziarie ai prestatori di servizi senza il previo coinvolgimento di altri Stati. La conseguenza di ciò è che ogni prestatore decide di volta in volta se collaborare ed entro che limiti: si parla pertanto di *voluntary disclosure*[11].

Si capisce perché, da tempo, le questioni connesse all'accesso di prove elettroniche dislocate al di fuori del territorio nazionale abbiano fatto il loro ingresso nelle corti di tutto il mondo e abbiano condizionato – e stiano condizionando – le scelte dei legislatori. Al riguardo, si pensi al famoso caso *Microsoft c. Stati Uniti*. Nel 2013, la Microsoft ricevette l'ordine da parte del Dipartimento di Giustizia degli Stati Uniti d'America di rendere disponibile una serie di *e-mail* relative a un certo account. Queste *e-mail* erano conservate in Irlanda, dunque al di fuori della giurisdizione degli Stati Uniti, e pertanto, secondo Microsoft, non sarebbe sussistito alcun obbligo quanto alla loro produzione sulla base della legge al tempo in vigore. A seguito di alterne vicende processuali, la controversia si è conclusa con l'emissione di un altro mandato, fondato su di una nuova disciplina adottata nel frattempo. Si tratta del *Clarifying Lawful Overseas Use of Data Act* (detto *CLOUD Act*), il quale permette alle autorità di *law enforcement* statunitensi di richiedere ai prestatori di servizi di conservare e produrre dati relativi ai loro clienti che siano archiviati al di fuori del territorio degli Stati Uniti[12].

Convenzione di Budapest del 2001, in *La Comunità Internazionale* 2001, 59 ss., M. Keyser, *The Council of Europe Convention on Cybercrime*, in *Journal of Transnational Law & Policy* 2002, 287 ss., A.M. Weber, *The Council of Europe's Convention on Cybercrime*, in *Berkeley Technology Law Journal* 2003, 425 ss. e J. Clough, *A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation*, in *Monash University Law Review* 2014, 698 ss. Sui profili di diritto interno, E. Colombo, *La cooperazione internazionale nella prevenzione e lotta alla criminalità informatica: dalla Convenzione di Budapest alle disposizioni nazionali*, in *Cyberspazio e diritto* 2009, 285 ss. e 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.

[11] M. Daniele, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Revista Brasileira de Direito Processual Penal* 2019, 1282. Peraltro, di tale realtà si dà atto anche nella Convenzione sulla criminalità informatica del Consiglio d'Europa. L'articolo 32 di quest'ultima prevede infatti che una Parte contraente possa accedere o ricevere, attraverso un sistema informatico nel proprio territorio, dati informatici immagazzinati in un altro Stato, se la Parte ottiene il consenso legale e volontario della persona legalmente autorizzata a divulgare i dati allo Stato attraverso tale sistema informatico, senza bisogno di ottenere il previo consenso dell'altro Stato.

[12] La causa portata dinanzi alla Corte Suprema è *United States v. Microsoft Corp.*, 584 U.S., 138 S. Ct. 1186 (2018). Riguardo agli sviluppi giurisprudenziali e legislativi ora riassunti, J. Daskal, *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, in *Stanford Law Review Online* 2018, 9 ss. ed E. Kyriakides, *The CLOUD Act, E-Evidence, and Individual Rights*, in *European Data Protection Law Review*, 2019, 99 ss.

Mentre il caso *Microsoft* era ancora pendente, la *California Northern District Court* ebbe modo di deciderne uno simile, relativo a due mandati emessi nei confronti di Google sulla base della normativa precedente al *CLOUD Act*. In quell'occasione, la *District Court* si pronunciò in senso favorevole al governo degli Stati Uniti, rilevando che, a prescindere dalla localizzazione delle informazioni, l'attività di indagine connessa ai dati che avrebbero dovuto essere prodotti si sarebbe svolta negli Stati Uniti, una volta che essi fossero stati resi disponibili[13].

Nel frattempo, il problema era emerso anche dall'altra parte dell'Atlantico e in più occasioni, negli ultimi anni, richieste di accesso a dati nella disponibilità di prestatori di servizi telematici sono state formulate da parte di autorità di Stati europei diversi da quelli in cui esse avevano la loro sede, il che ha portato a pronunce giurisprudenziali solitamente favorevoli alle autorità investigative[14] e a riforme a livello legislativo[15].

Anche l'Unione europea ha assunto delle iniziative in materia. Al riguardo, può farsi riferimento alla direttiva 2014/41 sull'ordine europeo di indagine penale (OEI)[16]. Come noto, quest'ultimo si configura come uno strumento di cooperazione giudiziaria in materia penale attraverso il quale l'autorità competente di uno Stato membro può compiere uno o più atti di indagine in un altro Stato membro ai fini dell'acquisizione di prove. Pur non prevedendo una disciplina specifica relativa alle prove elettroniche, va considerato che nel definirne l'ambito di applicazione l'articolo 3 della direttiva chiarisce che l'OEI può essere emesso per qualsiasi atto di indagine, tranne che per l'istituzione di una squadra investigativa comune e per l'acquisizione di prove nell'ambito di tale squadra. Dunque, la ricerca di *e-evidence* può sicuramente avvenire attraverso il meccanismo in parola.

---

[13] *In re Search Warrant No. 16-960-M-01 to Google*, 232 F. Supp. 3d 708 (2017).

[14] Sul tema, P. de Hert, M. Kopcheva, *International mutual legal assistance in criminal law made redundant: A comment on the Belgian Yahoo! case*, in *Computer Law & Security Review*, 2011, 291 ss. e J. Daskal, *Borders and Bits*, in *Vanderbilt Law Review* 2018, 179 ss.

[15] Quanto alle iniziative negli ordinamenti britannico e belga, L. Crooper, *The Investigatory Powers Act 2016 – A "Snoopers' Charter" or a legitimate surveillance tool for today's society?*, in www.fieldfisher.com, 02.04.2017 e V. Franssen, *The Belgian Internet Investigatory Powers Act - A Model to Pursue at European Level?*, in *European Data Protection Law Review* 2017, 534 ss.

[16] Direttiva 2014/41/UE del Parlamento europeo e del Consiglio del 3 aprile 2014 relativa all'ordine europeo di indagine penale, in GU L 130, 1.5.2014, 1, sulla quale L. Camaldo, *La direttiva sull'ordine europeo di indagine penale (OEI): un congegno di acquisizione della prova dotato di molteplici potenzialità, ma di non facile attuazione*, in *Diritto penale contemporaneo*, 27 maggio 2014, I. Armada, *The European Investigation Order and the Lack of European Standards for Gathering Evidence: Is a Fundamental Rights-Based Refusal the Solution?*, in *New Journal of European Criminal Law* 2015, 8 ss., R. Belfiore, *The European Investigation Order in Criminal Matters: Developments in Evidence-gathering across the EU*, in *European Criminal Law Review* 2015, 312 ss. e R. Jurka, *Movement of evidence in the European Union: Challenges for the European Investigation Order*, in *Baltic Journal of Law & Politics* 2016, 56 ss. Sugli aspetti inerenti all'entrata a regime dell'ordine europeo di indagine penale nell'ordinamento italiano, M. Daniele, R.E. Kostoris (a cura di), *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 198 del 2017*, Torino 2018.

È però stata avvertita con forza l'esigenza di definire una procedura specifica relativa a questo tipo di prove, come confermato, nel 2015, da parte della Commissione europea nell'Agenda europea sulla sicurezza. Secondo la Commissione, fermo il rispetto dovuto ai principi in materia di protezione dei dati personale, è necessario per le autorità giudiziarie e di polizia ottenere l'accesso a dati funzionali a tutelare la vita dei cittadini dalla criminalità informatica. A tal fine, la cooperazione con il settore privato è di primaria importanza[17]. Un'indicazione in questo senso è stata fornita, a seguito degli attentati terroristici di Bruxelles del 22 marzo 2016[18], anche da parte del Consiglio dell'Unione europea, il quale ha sollecitato la Commissione a formulare una proposta diretta a permettere la suddetta forma di cooperazione[19].

È stata così lanciata da parte dell'esecutivo europeo una consultazione pubblica al fine di comprendere quali fossero le prassi esistenti in materia di accesso transnazionale alle prove elettroniche negli Stati membri e i problemi di ordine giuridico e pratico riscontrati da parte dei diversi *stakeholder*[20]. All'esito di tale consultazione, la Commissione ha espresso l'intenzione di elaborare un quadro giuridico idoneo a permettere alle autorità competenti di obbligare un prestatore di servizi avente sede in un altro Stato membro a divulgare dati nella sua disponibilità[21].

Da parte sua, anche il Parlamento europeo ha manifestato sostegno rispetto a un'iniziativa del genere, sottolineando l'esigenza di un approccio comune alla giustizia penale nel cyberspazio, fondato su di uno strumento funzionale ad ottenere le prove elettroniche in maniera rapida, su di una stretta cooperazione tra le autorità di contrasto e i prestatori di servizi e su di un'adeguata protezione dei diritti e delle libertà dei diversi soggetti coinvolti[22].

Il 17 aprile 2018, infine, la Commissione europea ha pubblicato una proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in

[17] Commissione europea, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "Agenda europea sulla sicurezza", 28.04.2015, COM(2015) 185 final, 22.

[18] Come ricordato in Commissione europea, *Unione della sicurezza: la Commissione facilita l'accesso alle prove elettroniche*, 17.04.2018, in https://ec.europa.eu/commission/presscorner/detail/it/IP_18_3343.

[19] Consiglio dell'Unione europea, *Council conclusions on improving criminal justice in cyberspace*, 09.06.2016, 3.

[20] Si veda https://ec.europa.eu/info/consultations/public-consultation-improving-cross-border-access-electronic-evidence-criminal-matters_en.

[21] Commissione europea, *Inception Impact Assessment, Improving cross-border access to electronic evidence in criminal matters*, Ref. Ares. 2017 3896097 - 03/08/2017, 3.

[22] Risoluzione del Parlamento europeo del 3 ottobre 2017 sulla lotta alla criminalità informatica (2017/2068(INI)), punti 62-65.

materia penale[23] e una proposta di direttiva sulla nomina dei rappresentanti legali dei prestatori di servizi[24].

3. Attraverso la proposta di regolamento si mira a introdurre una disciplina unitaria relativa a due nuovi strumenti di cooperazione giudiziaria in materia penale: l'ordine europeo di produzione e l'ordine europeo di conservazione. Questi ordini verrebbero emessi nell'ambito di procedimenti penali avviati sia nei confronti di persone fisiche, sia nei confronti di persone giuridiche, tanto in fase preprocessuale, quanto in fase processuale, al fine di ottenere prove elettroniche o di imporne la conservazione – dunque, impedirne la rimozione, la cancellazione o la modifica in vista di una successiva richiesta di produzione – da parte di prestatori di servizi di comunicazione elettronica, della società dell'informazione (come nel caso dei social network e dei mercati online), di nomi di dominio Internet e di numerazione IP attivi nell'Unione europea.

Ai sensi dell'articolo 2, n. 6-10, si identificano come prove elettroniche le prove conservate in formato elettronico da parte del prestatore di servizi o per suo conto, che possono consistere in:

- dati relativi agli abbonati, ossia informazioni relative all'identità di un abbonato o di un cliente (per esempio, nome e data di nascita), al tipo di servizio e alla sua durata;
- dati relativi agli accessi, inerenti all'inizio e alla fine di una sessione di utilizzo da parte dell'utente, i quali possono riguardare data e ora di uso, il *log-in*, il *log-off* e il numero IP;
- dati relativi alle operazioni, che forniscono informazioni di contesto quanto al servizio utilizzato (per esempio, fonte e destinatario di un messaggio);
- dati relativi al contenuto, che si identificano in qualsiasi dato conservato in formato digitale, come testo, voce, video, immagine o suono, diverso dai dati relativi agli abbonati, agli accessi e alle operazioni.

[23] 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, 17.04.2018, sulla quale si possono vedere, oltre ai testi citati *infra*, S. Depauw, *Electronic Evidence in Criminal Matters: How About E-Evidence Instruments 2.0?*, in *European Criminal Law Review* 2018, 62 ss., G. Robinson, *The European Commission's e-Evidence Proposal*, in *European Data Protection Law Review* 2018, 347 ss., S. Tosza, *The European Commission's Proposal on Cross-Border Access to E-Evidence*, in *Eucrim* 2018, 212 ss., B.J. Blažič, T. Klobučar, *Removing the barriers in cross-border crime investigation by gathering e-evidence in an interconnected society*, in *Information & Communication Technology Law* 2020, 66 ss. e V. Tondi, *L'accesso transfrontaliero all'electronic evidence, tra esigenze di effettività e tutela dei diritti*, in *Diritto penale contemporaneo*, 2/2019, 439 ss.

[24] 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, 17.04.2018.

L'ordine europeo di produzione riguardante i dati relativi agli abbonati o agli accessi e l'ordine europeo di conservazione possono essere emessi da un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero. Ulteriormente, l'ordine può essere emesso da qualsiasi altra autorità dello Stato di emissione che agisca in qualità di autorità inquirente nel procedimento penale e sia competente a disporre l'acquisizione di prove in conformità del diritto nazionale ma in tal caso è richiesta la convalida da parte di un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero.

L'ordine europeo di produzione riguardante dati relativi alle operazioni o al contenuto può essere emesso da tutte le autorità ora menzionate, con l'eccezione del pubblico ministero.

Ai fini dell'emissione tanto dell'uno, quanto dell'altro ordine si impone una valutazione preliminare circa la necessità e la proporzionalità del provvedimento. Ai sensi dell'articolo 5, l'ordine di produzione di dati relativi agli abbonati e agli accessi può essere emesso per qualunque reato, mentre nel caso di dati relativi alle operazioni e al contenuto è necessario che l'ordine si ricolleghi a un reato punito nello Stato di emissione con una pena detentiva della durata massima di almeno tre anni o per reati in materia di frode e falsificazione dei mezzi di pagamento diversi dai contanti, abuso e sfruttamento sessuale di minori, pornografia infantile, attacchi contro i sistemi di informazione e terrorismo. Nel caso dell'ordine di produzione, l'autorità emittente può procedere solo se una misura dello stesso tipo risulta prevista dalla legislazione interna per lo stesso reato in una situazione nazionale comparabile.

Gli ordini sono diretti nei confronti del rappresentante legale del prestatore di servizi o, ove questi non sia designato, nei confronti di qualsiasi stabilimento del prestatore presente nel territorio dell'Unione, e vengono emessi nella forma di certificati contenenti una serie di informazioni relative, tra l'altro, all'autorità emittente, al soggetto i cui dati sono richiesti e al tipo di dati a cui accedere o da conservare.

A seguito della ricezione del certificato, il prestatore di servizi, nel caso dell'ordine di produzione, provvede alla trasmissione dei dati nel termine di dieci giorni, a meno che l'autorità emittente non abbia fatto valere ragioni di divulgazione anticipata; nel caso dell'ordine di conservazione, conserva, senza indebito ritardo, i dati richiesti. La conservazione non può protrarsi oltre il termine di sessanta giorni, a meno che l'autorità di emissione confermi che è stata avviata la successiva richiesta di produzione. In tale ipotesi, il prestatore di servizi conserva i dati per tutto il tempo necessario per la loro produzione una volta che la richiesta di produzione sia stata notificata.

Il destinatario dell'ordine è comunque tenuto ad assicurare la riservatezza del certificato e dei dati e, ove richiesto in tal senso da parte dell'autorità di emissione, non dà informazione di ciò al titolare dei dati, il quale però viene informato a seguito della produzione dei dati. Ciò può comunque essere posticipato per il tempo necessario e proporzionato a non ostacolare il procedimento penale.

Ai sensi dell'articolo 13, ferma la competenza nazionale a definire sanzioni penali, gli Stati membri provvedono a individuare sanzioni pecuniarie effettive, proporzionate e dissuasive applicabili ai casi di violazione degli obblighi di esecuzione degli ordini e di riservatezza.

Ove il destinatario non ottemperi all'ordine, senza fornire motivi che siano accettati dall'autorità di emissione, questa può richiedere l'intervento dell'autorità competente dello

Stato di esecuzione, la quale riconosce l'ordine e adotta le misure necessarie alla sua esecuzione, a meno che ritenga che si applichi uno dei motivi per i quali il destinatario può opporsi. Tali sono le ipotesi in cui:

- l'ordine non sia stato emesso o convalidato da un'autorità di emissione conformemente alla nozione individuata nel Regolamento;
- l'ordine europeo di produzione non sia stato emesso in relazione a un reato di cui all'articolo 5;
- il destinatario non abbia potuto ottemperare per impossibilità materiale o forza maggiore o perché il certificato contiene errori manifesti;
- l'ordine non riguardi dati conservati dal prestatore di servizi o per suo conto al momento della ricezione del certificato;
- il servizio esuli dall'ambito di applicazione del regolamento;
- si ritenga che l'ordine violi manifestamente la Carta dei diritti fondamentali dell'Unione europea o che sia manifestamente arbitrario.

Ulteriormente, l'autorità dello Stato di esecuzione non provvede se i dati sono protetti da un'immunità o un privilegio riconosciuti dal diritto nazionale o se la divulgazione può incidere su interessi fondamentali dello Stato (quali la sicurezza e la difesa nazionali). In ogni caso, la decisione sul riconoscimento è assunta entro cinque giorni lavorativi dalla ricezione dell'ordine.

Ove il destinatario si opponga, l'autorità di esecuzione decide se eseguire l'ordine sulla base delle informazioni fornite da quello e, se necessario, delle informazioni supplementari ottenute dall'autorità di emissione.

Se ritiene che l'ottemperanza all'ordine europeo di produzione sia in contrasto con il diritto applicabile di uno Stato terzo che vieta la divulgazione dei dati in questione per la necessità di tutelare i diritti fondamentali delle persone interessate o interessi fondamentali dello Stato terzo connessi alla sicurezza o alla difesa nazionali, il destinatario informa l'autorità di emissione, la quale riesamina l'ordine. Ove intenda confermarlo, ne chiede il riesame da parte dell'organo giurisdizionale competente del proprio Stato membro, che procede a una valutazione tenendo conto della disciplina dello Stato terzo e degli interessi che essa mira a tutelare. Se ritiene che non esista alcun contrasto, conferma l'ordine. In caso contrario, trasmette alle autorità centrali dello Stato terzo tutte le informazioni relative al caso, compresa la propria valutazione, fissando per rispondere un termine di quindici giorni, prorogabile di trenta. Se entro il termine stabilito l'autorità centrale dello Stato terzo comunica la propria opposizione all'esecuzione, l'organo giurisdizionale competente revoca l'ordine e ne informa l'autorità di emissione e il destinatario. Se non riceve alcuna opposizione, invia un sollecito, concedendo altri cinque giorni per rispondere e informandola delle conseguenze della mancata risposta. Qualora non riceva alcuna opposizione entro tale ulteriore termine, l'organo giurisdizionale competente conferma l'ordine e informa l'autorità di emissione e il destinatario, che deve procedere nell'esecuzione dell'ordine.

Nel caso in cui il destinatario ritenga che l'ordine di produzione sia in contrasto con il diritto applicabile di uno Stato terzo che vieta la divulgazione dei dati per motivi diversi da

quelli ora menzionati, la decisione è assunta dall'organo giurisdizionale competente dello Stato membro di emissione, senza il coinvolgimento delle autorità dello Stato terzo.

Indagati, imputati e altri soggetti i cui dati siano stati ottenuti tramite un ordine europeo di produzione hanno diritto a un ricorso effettivo, che può essere esercitato dinanzi a un organo giurisdizionale dello Stato di emissione.

La proposta di direttiva riguarda l'armonizzazione delle norme nazionali in materia di rappresentanti legali dei prestatori di servizi. Tramite essa si mira a fare sì che gli Stati membri obblighino i prestatori di servizi attivi nell'Unione, anche se non stabiliti nel territorio di questa, a individuare almeno un rappresentante legale ai fini della ricezione, dell'ottemperanza e dell'esecuzione di provvedimenti emessi dalle autorità competenti di ciascuno Stato membro a fini probatori. Il rappresentante legale deve risiedere o essere stabilito nel territorio di uno degli Stati membri in cui il prestatore svolge la propria attività ed è obbligato a cooperare con le autorità. A tal fine, egli gode dei poteri e delle risorse necessari e può essere ritenuto responsabile del mancato rispetto degli obblighi derivanti dalla disciplina in materia di ordini di produzione e di conservazione.

4. La presentazione della proposta da parte della Commissione europea ha suscitato un forte dibattito tanto nell'ambito del sistema istituzionale dell'Unione europea, quanto al di fuori di esso.

Il Comitato economico e sociale ha espresso un giudizio positivo, considerando che la direttiva sull'ordine europeo di indagine penale non contiene una disciplina specifica relativa alla raccolta di prove elettroniche e che la proposta della Commissione dovrebbe consentire di provvedere a ciò in maniera semplice e rapida. In particolar modo, è stato fatto presente che esistono delle differenze significative tra gli ordinamenti degli Stati membri quanto alle condizioni di accesso ai dati nell'ambito di un procedimento penale e quanto alle autorità competenti a decidere in materia. Il che renderebbe quanto mai necessario lo sviluppo di standard uniformi per quel che riguarda i presupposti di accesso[25].

Tuttavia, il Comitato economico e sociale ha segnalato come problematico il riconoscimento in favore del pubblico ministero del potere di emettere un ordine di produzione di dati relativi agli abbonati o agli accessi. Questo in quanto si tratta di dati personali e la tutela giuridica *ex post* nel caso di accesso da un altro Stato membro risulterebbe difficile[26].

Successivamente, il Consiglio dell'Unione europea ha proposto una serie di modifiche al testo della Commissione. In particolare, gli emendamenti di maggior rilievo riguardano:

[25] Parere del Comitato economico e sociale europeo sulla «Proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale» e sulla «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», in GU C 367, 10.10.2018, 88, punti 1.6 e 3.2.

[26] *Ibidem*, punti 1.7 e 3.10.

- l'ambito di applicazione del regolamento, che viene esteso anche alla fase dell'esecuzione di pene detentive nel caso in cui il condannato si sia sottratto alla giustizia;
- la possibilità per le autorità non giudiziarie di emettere un ordine senza convalida da parte di un'autorità giudiziaria in via eccezionale con riferimento a casi di emergenza adeguatamente accertata;
- il chiarimento quanto al fatto che l'ordine europeo di produzione diretto a ottenere dati relativi agli abbonati o agli accessi e l'ordine europeo di conservazione possano essere emessi ai fini dell'esecuzione di sanzioni detentive di durata di almeno quattro mesi;
- la specificazione che la trasmissione dei certificati e dei dati deve avvenire attraverso una modalità sicura e affidabile;
- la possibilità di informare il titolare dei dati nel caso in cui vi sia una richiesta in tal senso da parte dell'autorità emittente;
- l'affermazione di una sorta di principio di specialità, in forza del quale le prove elettroniche ottenute attraverso il ricorso all'ordine di produzione non possono essere utilizzate per finalità diverse da quelle connesse all'emissione di quell'ordine, a meno che non si tratti di farvi ricorso nell'ambito di procedimenti per reati elencati all'articolo 5 della proposta o al fine di prevenire una minaccia immediata e grave alla pubblica sicurezza dello Stato di emissione o ai suoi interessi essenziali[27];

[27] Si fa presente *en passant* che la scelta di rubricare la previsione in questione "Principio di specialità" appare alquanto curiosa. Notoriamente, nell'ambito delle procedure estradizionali l'affermazione del principio di specialità implica che il soggetto estradato non possa essere arrestato, processato e punito per un reato diverso rispetto a quello per il quale sia stata richiesta la sua estradizione. La ragione principale di ciò si ricollega all'esigenza di evitare che un soggetto, una volta consegnato, venga sottoposto a processo ed eventualmente a sanzioni per ragioni diverse da quelle che ne hanno giustificato il trasferimento, in particolar modo per reati politici (per un'introduzione al tema, J. George, *Toward a More Principled Approach to the Principle of Specialty*, in *Cornell International Law Journal* 1979, 310 ss., B. Bouloc, *Le principe de specialité en droit pénal international*, in *Mélanges dédiés à Dominique Holleaux*, Paris 1990, 7 ss., M.R. Marchetti, *L'estradizione: profili processuali e principio di specialità*, Padova 1990, D. Runtz, *The Principle of Specialty: A Bifurcated Analysis of the Rights of the Accused*, in *Columbia Journal of Transnational Law* 1991, 407 ss. e A. Zaïri, *Le principe de la spécialité de l'extradition au regard des droits de l'homme*, Paris 1992). Il principio in parola trova spazio anche nell'ambito di alcuni strumenti di cooperazione giudiziaria in materia penale dell'Unione europea (quali la decisione quadro 2002/584/GAI del Consiglio del 13 giugno 2002 relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri - Dichiarazioni di alcuni Stati membri sull'adozione della decisione quadro, in GU L 190, 18.7.2002, 1 e la decisione quadro 2008/909/GAI del Consiglio del 27 novembre 2008 relativa all'applicazione del principio del reciproco riconoscimento alle sentenze penali che irrogano pene detentive o misure privative della libertà personale, ai fini della loro esecuzione nell'Unione europea, in GU L 327, 5.12.2008, 27), per quanto siano previste eccezioni di rilievo alla sua applicazione, al fine di garantire l'efficienza dei meccanismi di cooperazione (sul tema, M. Caianiello, *Il principio di specialità*, in *Mandato d'arresto europeo. Dall'estradizione alle procedure di consegna*, a cura di M. Bargis, E. Selvaggi, Torino 2005, 213 ss., O. Lagodny, C. Rosbaud, *Speciality Rule*, in N. Keijzer, E. van Sliedregt (eds.), *The European Arrest Warrant in Practice*, The Hague 2009, 265 ss., E. Selvaggi, *Mandato d'arresto europeo e principio di specialità*, in *CP* 2009, 1296 ss. e S. Miettinen, *Onward Transfer under*

- l'applicazione di tale principio di specialità al fine di garantire il titolare dei dati contro la trasmissione degli stessi a uno Stato membro diverso da quello di emissione dell'ordine, il che può avvenire solo se si intende fare ricorso a quei dati nell'ambito di procedimenti per reati elencati all'articolo 5 della proposta o al fine di prevenire una minaccia immediata e grave alla pubblica sicurezza dello Stato membro o ai suoi interessi essenziali;
- la possibilità, in forza del principio di specialità, di condividere le prove elettroniche con Stati terzi od organizzazioni internazionali se l'ordine di produzione avrebbe potuto essere emesso in relazione al reato con riferimento al quale le prove sarebbero utilizzate e nel rispetto della direttiva 2016/680[28];
- l'obbligo per gli Stati di prevedere sanzioni amministrative pecuniarie per il mancato rispetto degli obblighi gravanti in capo al prestatore di servizi, le quali devono assumere la forma di una percentuale del fatturato complessivo annuo del prestatore di servizi a livello globale (2%);
- l'eliminazione della procedura di verifica prevista per il caso in cui l'ordine di produzione contrasti con la legge di uno Stato terzo in materia di diritti fondamentali dell'individuo o interessi fondamentali dello Stato e l'applicazione della procedura relativa alle altre ragioni anche a queste (con la conseguenza dunque che non sarebbe più previsto il coinvolgimento delle autorità centrali degli Stati terzi)[29].

Nello stesso mese, è stato pubblicato un report contenente una valutazione esterna richiesta da parte della Commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo. Le principali critiche rispetto alla proposta della Commissione europea si concentrano:

- sul mancato coinvolgimento di un'autorità giudiziaria nello Stato membro di esecuzione, il che porrebbe nelle mani di un privato la tutela dei diritti fondamentali;
- sul consequenziale arretramento rispetto al livello di tutela garantito dalla direttiva sull'ordine europeo di indagine penale;
- sulla mancata previsione di accordi bilaterali o multilaterali con Stati terzi, al fine di assicurare una migliore cooperazione e di risolvere il problema posto dall'esistenza di obblighi confliggenti derivanti dalla disciplina posta in altri ordinamenti giuridici;

---

the European Arrest Warrant: Is the EU Moving towards the Free Movement of Prisoners?, in *New Journal of European Criminal Law* 2013, 99 ss.).

[28] Si tratta della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, in GU L 119, 04.05.2016, 89.

[29] Consiglio dell'Unione europea, *Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters - general approach*, 11.06.2019, 10206/19.

- sulla mancata previsione di rimedi giudiziari esperibili da parte del prestatore di servizi nello Stato membro di esecuzione[30].

A queste critiche si sono aggiunte quelle degli *stakeholder* e della dottrina. I primi hanno segnalato i rischi connessi alla privatizzazione di funzioni tradizionalmente svolte da parte di autorità giudiziarie. Ciò riguarderebbe in particolar modo la valutazione dei profili di necessità e di proporzionalità degli ordini, rispetto alla quale si troverebbero impreparate soprattutto le piccole e medie imprese, non avendo esse le conoscenze e le competenze che una simile analisi richiede sul piano strettamente giuridico[31].

Ulteriormente, è stata posta in evidenza l'esigenza di assicurare un *right to notice* in favore del titolare dei dati, nonché di prevedere un'autorizzazione da parte dell'autorità giudiziaria dello Stato di esecuzione anteriormente a che il prestatore ottemperi all'ordine, di adottare accordi internazionali così da evitare conflitti di legge derivanti dai differenti regimi applicati nei vari ordinamenti giuridici e di assicurare la trasparenza dei meccanismi proposti dalla Commissione al fine di prevenire abusi e assicurare una forma di controllo da parte dell'opinione pubblica[32].

Da parte sua, la dottrina ha rilevato una serie di punti controversi[33], concentrando la propria attenzione su almeno tre aspetti significativi:

- la dubbia individuazione della base giuridica della proposta di regolamento nell'articolo 82, paragrafo 1, del Trattato sul Funzionamento dell'Unione europea: tale previsione, con la quale è stato "costituzionalizzato" il principio di riconoscimento reciproco delle sentenze e delle decisioni giudiziarie in materia penale[34], si configura come fondamento della cooperazione giudiziaria in ambito penale, dunque di una cooperazione che dovrebbe avere luogo tra autorità chiamate istituzionalmente a

[30] M. Böse, *An assessment of the Commission's proposals on electronic evidence*, Brussels 2018, 6.2.1-6.2.5. In sede di Parlamento europeo, sono stati in seguito presentati più di ottocento emendamenti rispetto alla proposta della Commissione (si veda https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=&reference=2018/0108(COD)#basicInformation).

[31] Così EuroISPA, *Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters. EuroISPA's considerations*, in https://www.euroispa.org/wp-content/uploads/1806_EuroISPA_e-evidence_position_paper.pdf, giugno 2018, 2. EuroISPA è un'organizzazione che rappresenta più di 2500 prestatori di servizi Internet in Europa.

[32] Così Brad Smith, presidente di Microsoft, in B. Smith, *A call for principle-based international agreements to govern law enforcement access to data*, in https://blogs.microsoft.com/on-the-issues/2018/09/11/a-call-for-principle-based-international-agreements-to-govern-law-enforcement-access-to-data/, 11.09.2018.

[33] Per una ricognizione complessiva, V. Franssen, *The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?*, in *European Law Blog*, 12.10.2018.

[34] Al riguardo, senza nessuna pretesa di esaustività, A. Suominen, *The Principle of Mutual Recognition in Cooperation in Criminal Matters*, Cambridge 2012, C. Janssens, *The Principle of Mutual Recognition in EU Law*, Oxford 2013, W. van Ballegooji, *The Nature of Mutual Recognition in European Law*, Cambridge, 2015 e L. Klimek, *Mutual Recognition of Judicial Decisions in European Criminal Law*, Berlin 2017.

svolgere una funzione giudiziaria; una simile qualifica, evidentemente, non può essere attribuita a un prestatore di servizi, ossia a un ente di diritto privato[35];

- l'evidente difficoltà derivante dal fatto di attribuire al prestatore di servizi il compito di valutare se l'ordine ricevuto si ponga in contrasto con gli obblighi derivanti dalla Carta dei diritti fondamentali dell'Unione europea e dall'articolo 6 del Trattato sull'Unione europea, dunque di richiedere a un privato di operare al fine della tutela dei diritti fondamentali come se fosse un'autorità giudiziaria[36];
- i problemi di coordinamento con la disciplina posta dalla direttiva sull'ordine europeo di indagine penale[37].

5. Ferme le critiche ora riassunte, vi è un ulteriore aspetto dubbio sul quale si intende concentrare l'attenzione e che attiene alla tecnica normativa alla quale si è fatto ricorso nella proposta di regolamento della Commissione europea.

In primo luogo, deve considerarsi che, come noto, un regolamento, inteso quale atto di diritto dell'Unione europea, risulta direttamente applicabile negli ordinamenti degli Stati membri. Non riconoscendo a questi ultimi la possibilità di determinare la disciplina rilevante, a esso è riconducibile un effetto di uniformazione, in quanto la stessa normativa è applicabile in tutti gli Stati dell'Unione.

Si tratta di una scelta – politica, prima ancora che giuridica – di non poco conto se si considera la storia della cooperazione giudiziaria in materia penale. Infatti, nel sistema delineato dal Trattato di Maastricht, essa rientrava nell'ambito del terzo pilastro, relativo alla Giustizia e Affari Interni, con la conseguenza che il metodo decisionale adottato era quello intergovernativo, fondato sulla riserva di sovranità statale. Tale stato di cose si rifletteva sugli atti all'epoca adottabili, individuati in azioni comuni, posizioni comuni e convenzioni. Mentre le prime due non risultavano vincolanti, alle terze era possibile ricondurre un effetto cogente solo a seguito della ratifica da parte degli Stati contraenti.[38].

A seguito della riforma operata con il Trattato di Amsterdam, ferme la collocazione della cooperazione giudiziaria in materia penale nel terzo pilastro e l'applicazione del metodo

[35] V. Mitsilegas, *The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence*, in *Maastricht Journal of European and Comparative Law* 2018, 263 ss.

[36] Al riguardo, E. Sellier, A. Weyembergh, *Criminal procedural laws across the European Union – A comparative analysis of selected main differences and the impact they have over the development of EU legislation*, Brussels 2018, 29-30 e N.A Smuha, *Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights & Consistency*, in *European Criminal Law Review* 2018, 83 ss.

[37] Su questo aspetto, oltre che sugli altri due precedenti, A. Rosanò, *La "privatizzazione" nello spazio di libertà, sicurezza e giustizia: tre esempi per una tendenza*, in *Il Diritto dell'Unione europea*, 2020, 179 ss.

[38] Per un'introduzione a questi temi, I.D. Hendry, *The Third Pillar of Maastricht: Cooperation in the Fields of Justice and Home Affairs*, in *German Yearbook of International Law* 1993, 295 ss., P.-C. Müller-Graf, *The Legal Basis of the Third Pillar and Its Position in the Framework of the Union Treaty*, in *Common Market Law Review* 1994, 493 ss., A. Tizzano, *Brevi note sul terzo pilastro del Trattato di Maastricht*, in *Il Diritto dell'Unione europea* 1996, 391 ss.

decisionale intergovernativo, si eliminò il riferimento alle azioni comuni e si aggiunse la possibilità di adottare decisioni quadro, ossia atti giuridicamente simili alle direttive alle quali. tuttavia non poteva essere attribuito alcun effetto diretto[39].

Con il Trattato di Lisbona, la struttura a pilastri dell'Unione è stata superata e si è assistito, *inter alia*, alla comunitarizzazione dell'ex terzo pilastro. Ciò ha comportato un cambiamento quanto al metodo decisionale applicato (che ora è quello comunitario, come per tutte le politiche dell'Unione, tranne la politica estera e di sicurezza comune) e quanto agli atti adottabili nell'ambito della cooperazione giudiziaria in materia penale[40].

Venuto meno il riferimento alle decisioni quadro, è ora possibile il ricorso a regolamenti e direttive. In questo senso e con riferimento all'articolo 82 TFUE, relativo agli aspetti più propriamente procedurali della cooperazione giudiziaria penale, deve segnalarsi quanto segue. Il paragrafo 2 menziona esclusivamente le direttive quali atti attraverso cui intervenire in materie quali l'ammissibilità reciproca delle prove tra gli Stati membri, i diritti della persona nella procedura penale, i diritti delle vittime della criminalità e altri elementi specifici della procedura penale, individuati dal Consiglio. Invece, il paragrafo 1, quanto alla definizione di norme e procedure dirette ad assicurare il riconoscimento in tutta l'Unione di sentenze e decisioni giudiziarie, alla prevenzione e risoluzione di conflitti di giurisdizione tra gli Stati membri, al sostegno alla formazione dei magistrati e degli operatori giudiziari e alla facilitazione della cooperazione tra le autorità giudiziarie od omologhe degli Stati membri in relazione all'azione penale e all'esecuzione delle decisioni, prevede solo che si ricorra alla procedura legislativa ordinaria quale procedura decisionale applicabile, senza individuare il tipo di atto adottabile.

Ciò legittima un intervento in materia anche mediante regolamenti. Una conferma al riguardo si ravvisa in un atto di recente approvazione: il regolamento 2018/1805 relativo al

[39] Per un'introduzione a questi temi, J. Monar, *Justice and Home Affairs in the Treaty of Amsterdam: Reform at the Price of Fragmentation*, in *European Law Review* 1998, 320 ss. e R. Adam, *La cooperazione in materia di giustizia e affari interni tra comunitarizzazione e metodo intergovernativo*, Milano 1999. Come noto, è tramite le decisioni quadro che sono stati raggiunti alcuni dei più significativi risultati sul piano della cooperazione giudiziaria in materia penale: valgano per tutti i riferimenti al mandato d'arresto europeo e alla procedura di trasferimento interstatale di detenuti.

[40] Per un'introduzione a questi temi, V. Mitsilegas, *EU Criminal Law after Lisbon. Rights, Trust and the Transformation of Justice*, Oxford 2016 e A. Weyembergh, *History of the Cooperation*, in R.E. Kostoris (ed.), *Handbook of European Criminal Procedure*, Cham, 2018, 173 ss.

riconoscimento reciproco dei provvedimenti di congelamento e di confisca[41], la cui base giuridica è identificata nell'articolo 82, paragrafo 1, lettera a), TFUE[42]. Dunque, l'intervento per via regolamentare è di certo possibile sulla base dell'articolo 82, paragrafo 1[43].

Questo aspetto è da valutarsi sicuramente in termini positivi *a valle*, dunque con riferimento al fatto che, una volta entrato in vigore il regolamento, varrà una stessa disciplina per tutti gli Stati membri dell'Unione e non si porranno problemi quanto a ritardi nel recepimento della fonte europea negli ordinamenti nazionali[44]. Al tempo stesso però si pongono dei problemi che devono essere affrontati *a monte*, dunque in sede di elaborazione del regolamento, e che si configurano come problemi di tecnica normativa. Proprio perché stesse regole si applicheranno in tutta l'Unione, è necessario che le previsioni siano quanto mai chiare e precise in modo da evitare interpretazioni divergenti a livello nazionale.

Allora, si capisce poco la decisione della Commissione europea di definire concetti chiave quali quelli di dati relativi agli abbonati, agli accessi, alle operazioni e al contenuto attraverso il ricorso a serie di ipotesi che non sembrano avere natura tassativa, ma meramente esemplificativa[45]. Tale scelta comporterebbe, nel caso in cui la proposta fosse approvata così com'è, il riconoscimento in favore dell'autorità giudiziaria emittente di un significativo margine interpretativo che permetterebbe di ampliare la platea dei dati a cui avere accesso. Il mancato coinvolgimento di un'autorità giudiziaria dello Stato membro di esecuzione ai fini della valutazione dell'ordine finirebbe così per porre sulle spalle del prestatore di servizi il compito di stabilire se i dati richiesti rientrino effettivamente nelle categorie contemplate dalla disciplina comunitaria oppure no[46].

Ulteriormente, la proposta della Commissione attribuisce agli Stati membri il compito di definire gli aspetti sanzionatori di carattere pecuniario. È infatti previsto che siano gli Stati

---

[41] Sul quale A.M. Maugeri, *Il regolamento (UE) 1805/2018 relativo al riconoscimento reciproco dei provvedimenti di congelamento e confisca: un importante passo in avanti in termini di cooperazione ed efficienza*, in *Diritto penale contemporaneo*, 04.12.2018 e A. Rosanò, *Congelamento e confisca di beni. Le novità del diritto dell'Unione europea nel quadro della cooperazione internazionale*, in *Eurojus.it*, 07.01.2019.

[42] Va comunque ricordato che nel preambolo del regolamento in parola, al punto 53, la Commissione europea specifica che "la forma giuridica del presente atto non dovrebbe costituire un precedente per i futuri atti giuridici dell'Unione nel settore del riconoscimento reciproco delle sentenze e delle decisioni giudiziarie in materia penale", aggiungendo che "la scelta della forma giuridica degli atti giuridici futuri dell'Unione dovrebbe essere valutata con attenzione caso per caso, tenendo conto, tra gli altri fattori, dell'efficacia dell'atto giuridico e dei principi di proporzionalità e sussidiarietà".

[43] Nel caso della proposta sulle *e-evidence*, però, deve ribadirsi la critica sopra menzionata quanto al fatto che si possa parlare di cooperazione giudiziaria quando una delle parti coinvolti non sia un'autorità giudiziaria. Il che renderebbe scorretta l'identificazione della base giuridica.

[44] Sottolineano questo aspetto 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 *Diritto penale contemporaneo*, 5/2018, 292.

[45] O. Pollicino, M. Bassini, *La proposta di Regolamento e-Evidence: osservazioni a caldo e possibili sviluppi*, in *Media Laws*, 26.10.2018.

[46] Dunque, si riproporrebbero in nuova veste i problemi sopra evidenziati quanto al ruolo dei prestatori quali soggetti di diritto privato nell'ambito di una procedura di cooperazione giudiziaria.

a stabilire sanzioni di questo tipo che siano effettive, proporzionate e dissuasive per il mancato rispetto da parte dei prestatori di servizi degli obblighi gravanti in capo a loro in forza del regolamento, ferma in ogni caso la loro competenza a individuare sanzioni penali. Il che può favorire un fenomeno di *forum shopping* da parte dei prestatori di servizi, al fine di evitare conseguenze eccessivamente gravose sul piano patrimoniale. Come detto *supra*, il Consiglio ha emendato questa previsione, proponendo di calcolare l'ammontare della sanzione in forza di una percentuale del fatturato annuo globale del prestatore di servizi. L'emendamento sembra andare nella giusta direzione se valutato in termini di uniformazione normativa.

Inoltre, non si è provveduto a introdurre una previsione idonea a uniformare la quantità di prove che possono essere richieste da parte dell'autorità emittente. L'assenza di un limite di ordine quantitativo potrebbe favorire la presentazione di richieste generiche, funzionali a ottenere quanti più dati possibile al fine di compensare eventuali carenze nell'attività delle autorità inquirenti.

Secondo alcuni, problemi sul piano dell'uniformazione deriverebbero anche dal fatto che non si sono chiarite le questioni attinenti all'ammissibilità delle prove conseguite illegalmente. Si pensi al caso, per esempio, di prove elettroniche ottenute sulla base di un ordine emesso da un'autorità giudiziaria non legittimata all'emissione di quel tipo di provvedimento. In questo caso, allora, la decisione dovrebbe essere assunta in forza di quanto previsto dalle singole legislazioni nazionali[47].

Il problema è di certo presente e deve essere segnalato. Tuttavia, potrebbe non essere possibile intervenire quanto a tale aspetto attraverso un regolamento. Infatti, l'ammissibilità reciproca delle prove tra gli Stati membri rientra tra le materie elencate all'articolo 82, paragrafo 2, con riferimento alle quali, come si diceva, è previsto un intervento normativo da parte dell'Unione solo attraverso le direttive.

6. Le proposte della Commissione europea sulla produzione e conservazione di *e-evidence* mirano a permettere di compiere un ulteriore passo in avanti sul piano della cooperazione giudiziaria in materia penale, introducendo una disciplina *ad hoc* che superi i modelli al momento esistenti e applicati nel contesto dell'Unione europea: da un lato, quello della *voluntary disclosure*, perché basato evidentemente ed esclusivamente sulla volontà del prestatore di servizi di collaborare; dall'altro, quello della direttiva sull'ordine europeo di indagine penale, che non terrebbe pienamente in conto della peculiare natura delle prove elettroniche quali informazioni che possono andare perdute con una certa facilità. Così, verrebbe a definirsi una sorta di *tertium genus* della cooperazione in materia, una sorta di *unvoluntary disclosure* che permetterebbe di superare tanto l'opposizione dei prestatori di servizi fondate sulla carenza di giurisdizione delle autorità emittenti, quanto il controllo dell'autorità dello Stato di esecuzione.

Anche in questo caso, allora, emergono le esigenze di efficienza che hanno condotto in passato all'adozione di altri strumenti di cooperazione giudiziaria nell'ordinamento

[47] V. Franssen, cit.

dell'Unione europea. Gli ordini di produzione e conservazione dovrebbero favorire lo svolgimento delle attività di ricerca della prova, almeno per quel che riguarda le prove elettroniche, in una maniera al tempo stesso più rapida e meno costosa[48]. Riecheggia in questo il mantra secondo cui la lotta alla criminalità passa per l'accesso veloce e semplice a quanti più dati possibile[49]. "Get access to lots of information at the lowest level of effort" è stato detto[50], e dunque possono comprendersi le ragioni che stanno alla base dell'iniziativa assunta da parte della Commissione europea.

Tuttavia, deve darsi atto di come, allo stato attuale, le proposte formulate – e, propriamente, la proposta di regolamento – possano essere intese solamente come testi di partenza alla luce dei quali condurre un approfondito dibattito sul tema.

Come confermano gli interventi di istituzioni e organi dell'Unione, degli *stakeholder* e della dottrina, sussistono criticità significative che si ricollegano in primo luogo al fatto di attribuire al prestatore di servizi – un privato – funzioni pubblicistiche, tradizionalmente svolte da parte delle autorità giudiziarie. Come in effetti non si è mancato di fare, possono sollevarsi dei dubbi quanto alla scelta di richiedere a un privato di svolgere attività di controllo che presuppongono una preparazione che difficilmente può ravvisarsi al di fuori del potere giudiziario.

Con il presente contributo si è inteso dare conto di un'ulteriore ragione di critica, relativa alla tecnica normativa utilizzata, la quale conferma la necessità di procedere a un'ulteriore riflessione sul tema della ricerca delle *e-evidence* in modo da evitare il sorgere di dubbi interpretativi in sede di applicazione della nuova disciplina, una volta approvata, e l'abbassamento degli standard di tutela dei diritti.

[48] L. Buono, *The genesis of the European Union's new proposed legal instrument(s) on e-evidence*, in *ERA Forum* 2019, 312.

[49] Parlano di mantra, G. González Fuster, S. Maymir Vazquez, *Cross-border Access to E-Evidence: Framing the Evidence*, CEPS Papers in Liberty and Security, 2020-02, 13.

[50] M.D. Cole, T. Quintel, *Transborder Access to e-Evidence by Law Enforcement Agencies. A first comparative view on the Commission's Proposal for a Regulation on a European Preservation/Production Order and accompanying Directive*, Université de Luxembourg, Law Working Paper Series, 2018-010, 18.