

C J N

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL
A QUARTERLY REVIEW FOR CRIMINAL JUSTICE



Nuove frontiere tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione e tecniche di prevenzione

IX Corso di formazione interdotto di Diritto e Procedura penale 'Giuliano Vassalli' per dottorandi e dottori di ricerca

(AIDP Gruppo Italiano, Siracusa International Institute for Criminal Justice and Human Rights – Siracusa, 29 novembre - 1° dicembre 2018)

ISSN 2240-7618

2/2019

EDITOR-IN-CHIEF

Gian Luigi Gatta

EDITORIAL BOARD

Italy: Antonio Gullo, Guglielmo Leo, Luca Luparia, Francesco Mucciarelli, Francesco Viganò
Spain: Jaime Alonso-Cuevillas, Sergi Cardenal Montraveta, David Carpio Briz, Joan Queralt Jiménez

Chile: Jaime Couso Salas, Mauricio Duce Julio, Héctor Hernández Basualto, Fernando Londoño Martínez

MANAGING EDITOR

Carlo Bray

EDITORIAL STAFF

Alberto Aimi, Enrico Andolfatto, Enrico Basile, Javier Escobar Veas, Stefano Finocchiaro, Elisabetta Pietrocarlo, Tommaso Trinchera, Stefano Zirulia

EDITORIAL ADVISORY BOARD

Rafael Alcacer Guirao, Alberto Alessandri, Giuseppe Amarelli, Ennio Amodio, Coral Arangüena Fanego, Lorena Bachmaier Winter, Roberto Bartoli, Fabio Basile, Hervé Belluta, Alessandro Bernardi, Carolina Bolea Bardón, David Brunelli, Silvia Buzzelli, Alberto Cadoppi, Pedro Caeiro, Michele Caianiello, Lucio Camaldo, Stefano Canestrari, Francesco Caprioli, Claudia Cárdenas Aravena, Raúl Carnevali, Marta Cartabia, Elena Maria Catalano, Mauro Catenacci, Massimo Ceresa Gastaldo, Mario Chiavario, Mirentxu Corcoy Bidasolo, Cristiano Cupelli, Norberto Javier De La Mata Barranco, Angela Della Bella, Cristina de Maglie, Gian Paolo Demuro, Miguel Díaz y García Conlledo, Ombretta Di Giovine, Emilio Dolcini, Jacobo Dopico Gomez Áller, Patricia Faraldo Cabana, Silvia Fernández Bautista, Javier Gustavo Fernández Terruelo, Marcelo Ferrante, Giovanni Fiandaca, Gabriele Fornasari, Novella Galantini, Percy García Caveró, Loredana Garlati, Mitja Gialuz, Glaucio Giostra, Víctor Gómez Martín, José Luis Guzmán Dalbora, Ciro Grandi, Giovanni Grasso, Giulio Illuminati, Roberto E. Kistoris, Máximo Langer, Juan Antonio Lascuráin Sánchez, María Carmen López Peregrín, Sergio Lorusso, Ezequiel Malarino, Francisco Maldonado Fuentes, Stefano Manacorda, Juan Pablo Mañalich Raffo, Vittorio Manes, Grazia Mannozi, Teresa Manso Porto, Luca Marafioti, Joseph Margulies, Enrico Marzaduri, Luca Masera, Jean Pierre Matus Acuña, Anna Maria Maugeri, Oliviero Mazza, Iván Meini, Alessandro Melchionda, Chantal Meloni, Melissa Miedico, Vincenzo Militello, Santiago Mir Puig, Fernando Miró Linares, Vincenzo Mongillo, Renzo Orlandi, Francesco Palazzo, Carlenrico Paliero, Michele Papa, Raphaële Parizot, Claudia Pecorella, Marco Pelissero, Lorenzo Picotti, Paolo Pisa, Oreste Pollicino, Domenico Pulitanò, Tommaso Rafaraci, Paolo Renon, Mario Romano, María Ángeles Rueda Martín, Carlo Ruga Riva, Stefano Ruggieri, Francesca Ruggieri, Marco Scoletta, Sergio Seminara, Paola Severino, Nicola Selvaggi, Rosaria Sicurella, Jesús María Silva Sánchez, Carlo Sotis, Giulio Ubertis, Inma Valeije Álvarez, Antonio Vallini, Paolo Veneziani, Costantino Visconti, Javier Willenmann von Bernath, Francesco Zacchè

Editore Associazione "Progetto giustizia penale", via Altavanguardia 1, Milano - c.f. 97792250157
ANNO 2019 - CODICE ISSN 2240-7618 - Registrazione presso il Tribunale di Milano, al n. 554 del 18 novembre 2011.
Impaginazione a cura di Chiara Pavesi

Diritto penale contemporaneo – Rivista trimestrale è un periodico on line ad accesso libero e non ha fine di profitto. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione. La rivista, registrata presso il Tribunale di Milano, al n. 554 del 18 novembre 2011, è edita attualmente dall'associazione "Progetto giustizia penale", con sede a Milano, ed è pubblicata con la collaborazione scientifica e il supporto dell'Università Commerciale Luigi Bocconi di Milano, dell'Università degli Studi di Milano, dell'Università di Roma Tre, dell'Università LUISS Guido Carli, dell'Universitat de Barcelona e dell'Università Diego Portales di Santiago del Cile.

La rivista pubblica contributi inediti relativi a temi di interesse per le scienze penalistiche a livello internazionale, in lingua italiana, spagnolo, inglese, francese, tedesca e portoghese. Ogni contributo è corredato da un breve abstract in italiano, spagnolo e inglese.

La rivista è classificata dall'ANVUR come rivista scientifica per l'area 12 (scienze giuridiche), di classe A per i settori scientifici G1 (diritto penale) e G2 (diritto processuale penale). È indicizzata in DoGI e DOAJ.

Il lettore può leggere, condividere, riprodurre, distribuire, stampare, comunicare al pubblico, esporre in pubblico, cercare e segnalare tramite collegamento ipertestuale ogni lavoro pubblicato su "Diritto penale contemporaneo – Rivista trimestrale", con qualsiasi mezzo e formato, per qualsiasi scopo lecito e non commerciale, nei limiti consentiti dalla licenza Creative Commons - Attribuzione - Non commerciale 3.0 Italia (CC BY-NC 3.0 IT), in particolare conservando l'indicazione della fonte, del logo e del formato grafico originale, nonché dell'autore del contributo.

La rivista può essere citata in forma abbreviata con l'acronimo: *DPC-RT*, corredato dall'indicazione dell'anno di edizione e del fascicolo.

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

La rivista si conforma alle norme del Regolamento UE 2016/679 in materia di tutela dei dati personali e di uso dei cookies ([clicca qui](#) per dettagli).

Ogni contributo proposto per la pubblicazione è preliminarmente esaminato dalla direzione, che verifica l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

In caso di esito positivo di questa prima valutazione, la direzione invia il contributo in forma anonima a due revisori, individuati secondo criteri di rotazione tra i membri dell'Editorial Advisory Board in relazione alla rispettiva competenza per materia e alle conoscenze linguistiche. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore.

La direzione comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se entrambe le valutazioni sono positive, il contributo è pubblicato. Se una o entrambe le valutazioni raccomandano modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se uno o entrambi i revisori esprimono parere negativo alla pubblicazione.

La direzione si riserva la facoltà di pubblicare, in casi eccezionali, contributi non previamente sottoposti alla procedura di peer review. Di ciò è data notizia nella prima pagina del contributo, con indicazione delle ragioni relative.

Se desideri proporre una pubblicazione alla nostra rivista, invia una mail a editor.criminaljusticenetwork@gmail.com. I contributi che saranno ritenuti dalla direzione di potenziale interesse per la rivista saranno sottoposti alla procedura di peer review sopra descritta. I contributi proposti alla rivista per la pubblicazione dovranno rispettare i criteri redazionali [scaricabili qui](#).



Diritto penale contemporaneo – Rivista trimestrale es una publicación periódica *on line*, de libre acceso y sin ánimo de lucro. Todas las colaboraciones de carácter organizativo y editorial se realizan gratuitamente y no se imponen a los autores costes de maquetación y publicación. La Revista, registrada en el Tribunal de Milan, en el n. 554 del 18 de noviembre de 2011, se edita actualmente por la asociación “Progetto giustizia penale”, con sede en Milán, y se publica con la colaboración científica y el soporte de la *Università Commerciale Luigi Bocconi* di Milano, la *Università degli Studi di Milano*, la *Università di Roma Tre*, la *Università LUISS Guido Carli*, la *Universitat de Barcelona* y la *Universidad Diego Portales de Santiago de Chile*.

La Revista publica contribuciones inéditas, sobre temas de interés para la ciencia penal a nivel internacional, escritas en lengua italiana, española, inglesa, francesa, alemana o portuguesa. Todas las contribuciones van acompañadas de un breve abstract en italiano, español e inglés.

El lector puede leer, compartir, reproducir, distribuir, imprimir, comunicar a terceros, exponer en público, buscar y señalar mediante enlaces de hipervínculo todos los trabajos publicados en “Diritto penale contemporaneo – Rivista trimestrale”, con cualquier medio y formato, para cualquier fin lícito y no comercial, dentro de los límites que permite la licencia *Creative Commons – Attribuzione – Non commerciale 3.0 Italia* (CC BY-NC 3.0 IT) y, en particular, debiendo mantenerse la indicación de la fuente, el logo, el formato gráfico original, así como el autor de la contribución.

La Revista se puede citar de forma abreviada en el acrónimo *DPC-RT*, indicando el año de edición y el fascículo.

La Revista asume el [Code of Conduct and Best Practice Guidelines for Journal Editors](#) elaborado por el COPE (*Comitte on Publication Ethics*).

La Revista cumple lo dispuesto en el Reglamento UE 2016/679 en materia de protección de datos personales ([clica aquí](#) para los detalles sobre protección de la privacy y uso de cookies).

Todas las contribuciones cuya publicación se propone serán examinadas previamente por la Dirección, que verificará la correspondencia con los temas tratados en la Revista y el respeto de los requisitos mínimos para su publicación.

En el caso de que se supere con éxito aquella primera valoración, la Dirección enviará la contribución de forma anónima a dos evaluadores, escogidos entre los miembros del *Editorial Advisory Board*, siguiendo criterios de rotación, de competencia por razón de la materia y atendiendo también al idioma del texto. Los evaluadores recibirán un formulario, que deberán devolver a la Dirección en el plazo indicado. En el caso de que la devolución del formulario se retrase o no llegara a producirse, la Dirección se reserva la facultad de escoger un nuevo evaluador.

La Dirección comunicará el resultado de la evaluación al autor, garantizando el anonimato de los evaluadores. Si ambas evaluaciones son positivas, la contribución se publicará. Si alguna de las evaluaciones recomienda modificaciones, la contribución se publicará después de que su autor la haya revisado sobre la base de los comentarios recibidos y de que la Dirección haya verificado que tales comentarios han sido atendidos. La contribución no se publicará cuando uno o ambos evaluadores se pronuncien negativamente sobre su publicación.

La Dirección se reserva la facultad de publicar, en casos excepcionales, contribuciones que no hayan sido previamente sometidas a *peer review*. Se informará de ello en la primera página de la contribución, indicando las razones.

Si deseas proponer una publicación en nuestra revista, envía un mail a la dirección editor.criminaljusticenetwork@gmail.com. Las contribuciones que la Dirección considere de potencial interés para la Revista se someterán al proceso de *peer review* descrito arriba. Las contribuciones que se propongan a la Revista para su publicación deberán respetar los criterios de redacción (se pueden [descargar aquí](#)).



Diritto penale contemporaneo – Rivista trimestrale is an on-line, open-access, non-profit legal journal. All of the organisational and publishing partnerships are provided free of charge with no author processing fees. The journal, registered with the Court of Milan (n° 554 - 18/11/2011), is currently produced by the association “Progetto giustizia penale”, based in Milan and is published with the support of Bocconi University of Milan, the University of Milan, Roma Tre University, the University LUISS Guido Carli, the University of Barcelona and Diego Portales University of Santiago, Chile.

The journal welcomes unpublished papers on topics of interest to the international community of criminal scholars and practitioners in the following languages; Italian, Spanish, English, French, German and Portuguese. Each paper is accompanied by a short abstract in Italian, Spanish and English.

Visitors to the site may share, reproduce, distribute, print, communicate to the public, search and cite using a hyperlink every article published in the journal, in any medium and format, for any legal non-commercial purposes, under the terms of the Creative Commons License - Attribution – Non-commercial 3.0 Italy (CC BY-NC 3.0 IT). The source, logo, original graphic format and authorship must be preserved.

For citation purposes the journal’s abbreviated reference format may be used: *DPC-RT*, indicating year of publication and issue.

The journal strictly adheres to the [Code of Conduct and Best Practice Guidelines for Journal Editors](#) drawn up by COPE (Committee on Publication Ethics).

The journal complies with the General Data Protection Regulation (EU) 2016/679 (GDPR) ([click here](#) for details on protection of privacy and use of cookies).

All articles submitted for publication are first assessed by the Editorial Board to verify pertinence to topics addressed by the journal and to ensure that the publication’s minimum standards and format requirements are met.

Should the paper in question be deemed suitable, the Editorial Board, maintaining the anonymity of the author, will send the submission to two reviewers selected in rotation from the Editorial Advisory Board, based on their areas of expertise and linguistic competence. The reviewers are provided with a feedback form to compile and submit back to the editorial board within an established timeframe. If the timeline is not heeded to or if no feedback is submitted, the editorial board reserves the right to choose a new reviewer.

The Editorial Board, whilst guaranteeing the anonymity of the reviewers, will inform the author of the decision on publication. If both evaluations are positive, the paper is published. If one or both of the evaluations recommends changes the paper will be published subsequent to revision by the author based on the comments received and verification by the editorial board. The paper will not be published should one or both of the reviewers provide negative feedback.

In exceptional cases the Editorial Board reserves the right to publish papers that have not undergone the peer review process. This will be noted on the first page of the paper and an explanation provided.

If you wish to submit a paper to our publication please email us at editor.criminaljusticenetwork@gmail.com. All papers considered of interest by the editorial board will be subject to peer review process detailed above. All papers submitted for publication must abide by the editorial guidelines ([download here](#)).

L'accesso transfrontaliero all'*electronic evidence*, tra esigenze di effettività e tutela dei diritti

*El acceso transfronterizo a evidencia electrónica,
entre exigencias de efectividad y tutela de derechos*

*Transnational Access to Electronic Evidence
Between Effectiveness and the Need to Protect Rights*

VERONICA TONDI

Dottoranda di ricerca presso la LUISS Guido Carli
vtondi@luiss.it

DIRITTI FONDAMENTALI,
INTERCETTAZIONI

DERECHOS FUNDAMENTALES,
INTERCEPTACIÓN DE COMUNICACIONES

FUNDAMENTAL RIGHTS, INTRUSIVE
SURVEILLANCE

ABSTRACTS

Il contributo si propone di prendere in esame i profili più significativi legati all'accesso transfrontaliero alla prova digitale, di crescente rilevanza in considerazione delle odierne tensioni tra limitazione della giurisdizione statale entro i confini nazionali e dematerializzazione dei dati informatici, non agevolmente collocabili in un determinato ambito territoriale. Oggetto di trattazione sono specificamente le recenti proposte di Regolamento e di Direttiva dell'Unione europea in materia di ordini europei di produzione e di conservazione dell'*electronic evidence*, considerati anche nel loro inquadramento nell'ambito del sistema normativo vigente, con particolare riguardo alle previsioni in materia di ordine europeo di indagine. Ad una sintetica analisi delle principali questioni relative ai rapporti tra l'Unione europea e Stati terzi in materia di accesso alla prova digitale seguono quindi alcune considerazioni conclusive sul nuovo modello di cooperazione fondato sul contatto diretto con il privato prestatore di servizi non sottoposto alla giurisdizione dello Stato procedente, in assenza, in linea di principio, di intermediazioni.

El presente trabajo tiene por objeto examinar las principales cuestiones relacionadas con el acceso transfronterizo a evidencia electrónica, tema de creciente relevancia en consideración a la problemática interacción entre la limitación de la jurisdicción estatal y la desmaterialización de los datos informáticos. El artículo aborda principalmente las recientes propuestas de reglamento y directiva de la Unión Europea en materia de ordenes europeas de producción y conservación de evidencia electrónica. A continuación, se analizan algunos de los principales problemas relativos a la relación entre la Unión Europea y terceros estados en asuntos de acceso transfronterizo a evidencia electrónica. Posteriormente, se efectúan algunas consideraciones finales sobre el nuevo modelo de cooperación directa con los proveedores de servicios de internet establecidos fuera de la jurisdicción estatal.

This paper aims to examine the most important issues involved by transnational access to electronic evidence. The latter is increasingly important due to the problematic interaction between the limitation of State jurisdiction within national boundaries and the dematerialization of data usable as evidence in criminal proceedings. The work mainly deals with the recent proposals of EU Regulation and Directive on European Production and Conservation Orders, aiming to analyse also their interference with the current law on judicial cooperation in criminal matters, especially with regard to the European Investigative Order. Some of the main problems concerning the relationship between the European Union and third States concerning transnational access to electronic evidence,

are then briefly examined, and followed by some final remarks on the new model of direct cooperation with service providers established outside the State jurisdiction.

SOMMARIO

1. Premessa. – 2. L'accesso transfrontaliero all'*electronic evidence* nell'ambito dell'Unione europea: le proposte di Regolamento e di Direttiva in materia di *European Production Order* e *European Preservation Order*. – 3. Ordine europeo di produzione, ordine europeo di conservazione, ordine europeo di indagine. – 4. Le caratteristiche fondamentali delle proposte normative. – 4.1. Dal mutuo riconoscimento al contatto diretto con il privato stabilito in altra giurisdizione. – 4.2. I destinatari degli ordini europei di produzione e di conservazione. – 4.3. I tempi delle procedure. – 4.4. Profili attinenti alla tutela dei diritti. – 4.5. I mezzi di impugnazione. – 5. La cooperazione con i *service providers* stabiliti in Stati terzi: il caso degli Stati Uniti. – 6. Il progetto di un secondo protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica: cenni. – 7. Considerazioni conclusive.

1.

Premessa.

Lo stretto intreccio tra nuove tecnologie e fenomeni criminali, l'esigenza di rendere i dispositivi e i sistemi informatici oggetto delle attività di indagine e istruttorie volte all'acquisizione di elementi di prova, e la necessità di avvalersi delle opportunità offerte dal progresso tecnico per le finalità della giustizia penale¹, appaiono ormai acquisizioni incontestabili.

Tali sistemi costituiscono invero, in misura crescente, tanto gli strumenti impiegati per la commissione di reati, quanto, e conseguentemente, la sede di conservazione di rilevanti dati e informazioni suscettibili di assumere valenza probatoria.

Il carattere immateriale dei dati, la loro agevole trasferibilità da un *server* a un altro, la mobilità degli strumenti utilizzati per la loro conservazione, così come l'utilizzo di tecnologie quali il *cloud computing*, idonei a comportare la scissione delle risorse da un supporto fisico e la loro diffusione in diversi sistemi e Paesi, non sempre agevolmente individuabili, oltre che la possibilità di una loro gestione ad opera di differenti *providers*², pongono problemi nuovi e particolarmente significativi nello svolgimento delle attività di indagine, di ricerca e di assunzione della prova, e sovente l'esigenza di un accesso alla cd. *electronic evidence* a carattere transfrontaliero.

In proposito, le questioni legate all'accesso a quest'ultima appaiono inserite nel più ampio problema dell'acquisizione della prova all'estero, alla luce del fatto che, mentre tanto le attività economiche, quanto quelle criminose eccedono in misura crescente i confini nazionali, significative differenze tra le normative nazionali in materia di assunzione e utilizzabilità della prova, sono frequentemente di ostacolo all'utilizzo della stessa quando essa sia assunta all'estero, secondo regole diverse da quelle dell'ordinamento di riferimento.

In tale ambito, tradizionalmente regolato da trattati internazionali, si sono inseriti significativi interventi normativi dell'Unione europea, tesi ad agevolare la circolazione della prova nello spazio giudiziario europeo e a rendere più agevole la cooperazione internazionale, secondo modalità tali da superare il modello della rogatoria, caratterizzato dall'intervento di autorità "centrali", a carattere amministrativo, sebbene l'intervento del ministro della giustizia sia stato già fortemente ridimensionato dalla Convenzione di assistenza giudiziaria del 2000. Si pone poi la questione della preferibilità di un approccio che sia tale da realizzare il mutuo riconoscimento dei provvedimenti adottati dagli Stati membri, o di un'impostazione che invece valorizzi l'armonizzazione delle disposizioni normative nazionali.

Gli strumenti previsti dal diritto vigente, disciplinati dal diritto dell'Unione europea e recepiti nell'ordinamento interno, che vanno nella direzione dell'incremento dell'efficienza e della rapidità della cooperazione tra Stati membri in materia di ricerca e acquisizione della prova sono rappresentati dalle squadre investigative comuni - regolate dalla Convenzione di Bruxelles in materia di assistenza giudiziaria del 2000 e dalla decisione quadro 2002/465/GAI, a cui è stata data attuazione in Italia solo con il d. lgs. 34/2016 - e dall'ordine europeo di indagine penale, introdotto dalla Direttiva 2014/41/UE, a cui è stata data attuazione nel nostro ordinamento con il d. gs. 21 giugno 2017, n. 108. Si deve altresì avere riguardo ai profili di transnazionalità delle attività di indagine connessi all'istituzione della Procura europea, con

¹ Sul sempre più frequente impiego, da parte dell'autorità giudiziaria, di strumenti investigativi a elevato contenuto tecnologico v. CERQUA Federico (2016), p. 96. In materia di prova digitale v. DI PAOLO Gabriella (2013), pp. 736-762.

² Cfr. PITTIRUTI Marco (2017).

Regolamento 2017/1939, in relazione ai reati che offendano gli interessi finanziari dell'U.E.³.

Deve peraltro ricordarsi come l'Unione europea abbia stipulato accordi con Stati terzi, quali U.S.A. e Giappone, in materia di assistenza giudiziaria⁴.

Il presente lavoro, pur incentrato sugli strumenti normativi dell'Unione, accennerà altresì al progetto relativo a un secondo protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica⁵, anch'esso, come si vedrà, teso a superare alcune criticità relative all'accesso transfrontaliero alla prova digitale.

2. L'accesso transfrontaliero all'*electronic evidence* nell'ambito dell'Unione europea: le proposte di Regolamento e di Direttiva in materia di *European Production Order* e *European Preservation Order*.

Le recenti proposte di Regolamento⁶ e di Direttiva⁷, elaborate dalla Commissione, in materia di accesso transfrontaliero all'*electronic evidence*, esprimono l'esigenza di superare anche quei profili di criticità e quei rallentamenti caratterizzanti procedure pur "agili" quali quelle suindicate, adattando «i meccanismi di cooperazione all'era digitale, fornendo alle autorità giudiziarie e di contrasto gli strumenti per stare al passo con le attuali modalità di comunicazione dei criminali e combattere le forme moderne di criminalità», assicurando al contempo «forti meccanismi di tutela dei diritti fondamentali»⁸. Esse rispondono altresì agli auspici formulati nelle Conclusioni del Consiglio dell'Unione europea sul miglioramento della giustizia penale nel ciber spazio⁹, del 2016, relativi all'incremento dell'efficienza dell'assistenza giudiziaria, al miglioramento della cooperazione tra le competenti autorità degli Stati membri e i prestatori di servizi stabiliti in Paesi terzi, nonché alla più chiara determinazione dei profili di territorialità legati allo svolgimento di indagini nel ciber spazio.

Le proposte appena menzionate, il cui iter formativo ha avuto inizio già con l'Agenda sulla sicurezza della Commissione del 2015 e ha subito una scossa soprattutto dopo gli attentati di Bruxelles del 2016¹⁰, prendono in primo luogo atto del fatto che, oggi, oltre la metà dei procedimenti penali implica esigenze di accesso transfrontaliero alla prova digitale, comprensiva, quest'ultima, a titolo esemplificativo e secondo le indicazioni della stessa istituzione, di sms, e-mail, messaggistica scambiata attraverso apposite applicazioni, quali *Whatsapp*¹¹. La definizione di "prova elettronica" è contenuta nella stessa proposta di Regolamento, all'art. 2, che riconduce a tale nozione «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»¹².

Le citate proposte intendono quindi introdurre nuovi strumenti di cooperazione finalizzati all'acquisizione dell'*electronic evidence* secondo modalità rapide ed efficaci; si tratta, in

³ V. in proposito RUGGERI (2018), p. 602.

⁴ Ne sono un esempio la Decisione 2009/820/PESC del Consiglio, del 23 ottobre 2009, relativa alla conclusione, a nome dell'Unione europea, dell'accordo sull'estradizione tra l'Unione europea e gli Stati Uniti d'America e dell'accordo sulla mutua assistenza giudiziaria tra l'Unione europea e gli Stati Uniti d'America, e la Decisione 2010/616/UE del Consiglio, del 7 ottobre 2010, relativa alla conclusione dell'accordo tra l'Unione europea e il Giappone sull'assistenza giudiziaria reciproca in materia penale.

⁵ Convenzione sulla criminalità informatica, aperta alla firma a Budapest il 23 novembre 2001.

⁶ Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale, 17 aprile 2018. Nella stessa Relazione illustrativa si dà atto della riconducibilità della scelta dello strumento del regolamento all'esigenza di predisporre -considerate le differenze anche significative ravvisabili tra gli ordinamenti dello Stato da cui provenga la richiesta e di quello di stabilimento del *service provider* - regole uniformi, necessarie quando vengano in considerazione procedure transfrontaliere, non apparendo opportuno lasciare agli Stati margini di apprezzamento nella loro attuazione.

⁷ 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, 17 aprile 2018.

⁸ Proposta di Regolamento, cit., 2.

⁹ Conclusioni del Consiglio dell'Unione europea sul miglioramento della giustizia penale nel ciber spazio, 9 giugno 2016, in www.data.consilium.europa.eu.

¹⁰ Cfr., per un commento alle due proposte in esame, GIALUZ Mitja, DELLA TORRE Jacopo (2018), p. 277 ss.; PEZZUTO Raffaella (2019), pp. 57-88.

¹¹ COMMISSIONE EUROPEA, *E-evidence - cross-border access to electronic evidence*, in www.ec.europa.eu.

¹² V. Proposta di Regolamento, cit., art. 2.

primo luogo, dell'ordine europeo di produzione (*European Production Order*), tale da consentire l'instaurazione di un contatto diretto tra l'autorità giudiziaria di uno Stato membro e il *service provider* che non sia stabilito entro i confini propri della giurisdizione del primo, e in particolare con il suo rappresentante, obbligatoriamente designato da chi presta i propri servizi all'interno dell'Unione, ma non sia stabilito in uno Stato membro. A tale istituto dovrebbe inoltre affiancarsi l'ordine europeo di conservazione (*European Preservation Order*), tale da porre in capo al *provider* un obbligo di conservazione di dati ed elementi di prova per un certo periodo di tempo, nella prospettiva di una futura acquisizione degli stessi attraverso gli strumenti di assistenza giudiziaria previsti.

Non estraneo ai progetti normativi in esame – e anzi all'interno degli stessi espressamente contemplato – è l'intento di unire al perseguimento dei menzionati obiettivi di efficienza la previsione di un elevato livello di garanzie, connesse specialmente alla tutela della riservatezza dei dati conservati e trasmessi.

3. Ordine europeo di produzione, ordine europeo di conservazione, ordine europeo di indagine.

Operata tale premessa in ordine alle caratteristiche essenziali delle proposte normative in esame, appare opportuno procedere alla definizione dei rapporti con gli altri strumenti di cooperazione, in materia di ricerca e acquisizione della prova, già contemplati dal diritto dell'Unione europea, e in particolare con il recente istituto dell'ordine europeo di indagine (*European Investigation Order*)¹³, introdotto dalla Direttiva 2014/41/UE, a cui è stata data attuazione nel nostro ordinamento con il d.lgs. 21 giugno 2017, n. 108, e considerato come la più avanzata disciplina in materia di raccolta transnazionale della prova mai adottata dal legislatore europeo, in quanto tale da rendere più rapida, snella e agevole la cooperazione tra Stati membri in materia¹⁴.

In primo luogo, la stessa proposta di Regolamento oggetto di esame chiarisce¹⁵ che la disciplina in materia di ordine europeo di indagine, applicabile ad ogni tipo di atto di indagine e probatorio¹⁶, e quindi anche alla prova digitale, seppure non contenente apposite disposizioni relative a quest'ultima, rimarrà in vigore per tutti quei profili non specificamente disciplinati dalla nuova normativa; l'inopportunità di una modifica della Direttiva in materia di OEI è motivata proprio dall'estensione di quest'ultima a una pluralità di tipologie di atti probatori.

Invero, a titolo esemplificativo, con riguardo alle informazioni oggetto di acquisizione per le finalità della giustizia penale, il nuovo disegno normativo si riferisce espressamente ai soli dati – considerati in una prospettiva “statica” – conservati dal *provider*, e non anche alle intercettazioni di flussi di comunicazioni, che continuano pertanto a rientrare nell'ambito di applicazione delle disposizioni in materia di ordine europeo di indagine¹⁷.

Giova altresì ricordare la possibile operatività, anche rispetto ai reati informatici di cui all'art. 51, comma 3-*quinquies*, c.p.p., delle disposizioni in materia di squadre investigative comuni¹⁸.

¹³ Di seguito indicato anche come “OEI”.

¹⁴ ALLEGREZZA Silvia, MOSNA Anna, NICOLICCHIA Fabio (2016), pp. 185-186.

¹⁵ In questo senso la Relazione illustrativa della proposta di Regolamento.

¹⁶ V. il considerando n. 6 della Direttiva, che, nel richiamare il Programma di Stoccolma del Consiglio UE del 10-11 dicembre 2009, fa riferimento all'auspicata «creazione di un sistema globale in sostituzione di tutti gli strumenti esistenti nel settore, compresa la decisione quadro 2008/978/GAI del Consiglio, che contempra per quanto possibile tutti i tipi di prove, stabilisca i termini di esecuzione e limiti al minimo i motivi di rifiuto». L'art. 3 del medesimo atto normativo specifica che non rientrano nell'ambito di applicazione della disciplina in materia di OEI solo l'istituzione di una squadra investigativa comune e gli atti di indagine dalla stessa compiuti. Proprio in ragione dell'aspirazione di completezza riferibile alla normativa in materia di OEI, essa ha sostituito la Convenzione europea di assistenza giudiziaria del 1959 e i relativi protocolli, la Convenzione di applicazione dell'accordo di Schengen del 1990, la Convenzione relativa all'assistenza giudiziaria in materia penale dell'Unione del 2000, recepita dal d. lgs. 5 aprile 2017, n. 52, e la decisione-quadro 2003/577 sul sequestro probatorio. Lo strumento della rogatoria continua tuttavia a trovare applicazione nei rapporti con gli Stati membri che non abbiano attuato la Direttiva (Irlanda e Danimarca) e con gli Stati non U.E.: v. BELFIORE Rosanna (2015), p. 3289; DANIELE Marcello (2017), p. 208; MANGIARACINA Annalisa (2018), p. 159.

¹⁷ V. in particolare gli artt. 23-24 e 43-44 del decreto legislativo di attuazione della Direttiva sull'OEI, in materia di “ordine di intercettazione” rispettivamente ricevuto ed emesso dall'autorità giudiziaria italiana. Sul tema, NOCERA Fabio (2018), pp. 149-168.

¹⁸ Disciplinate dalla decisione quadro 2002/465/GAI, attuata nell'ordinamento italiano con il d.lgs. 15 febbraio 2016, n. 34.

4. Le caratteristiche fondamentali delle proposte normative.

4.1. *Dal mutuo riconoscimento al contatto diretto con il privato stabilito in altra giurisdizione.*

La proposta di Regolamento sugli ordini europei di produzione e conservazione, al pari delle normative in materia di ordine europeo di indagine e di squadre investigative comuni, è dichiaratamente ispirata al principio del mutuo riconoscimento, di cui all'art. 82 del Trattato sul Funzionamento dell'Unione europea¹⁹. Difatti – sebbene, con riferimento all'ordine europeo di indagine, si sia posto in luce²⁰ come tale principio non risulti integralmente attuato, in ragione della previsione da parte della Direttiva, e del decreto di attuazione, di motivi di non riconoscimento dell'OEI o di rinvio dello stesso – lo strumento di cooperazione da ultimo indicato è tale da comportare un diretto contatto tra le autorità degli Stati membri, in assenza, come detto, dell'intervento di istituzioni centrali, frequentemente fonte di ritardi e inefficienze²¹.

Nel caso delle squadre investigative comuni, si configura addirittura l'operatività della squadra, all'interno di un determinato Stato membro, alla stregua di autorità del medesimo Stato²².

Pertanto, il profilo realmente innovativo dell'ordine europeo di produzione e dell'ordine europeo di conservazione è costituito dalla previsione di un contatto diretto tra l'autorità giudiziaria di uno Stato membro e il privato stabilito in altro Stato membro – identificabile, ai sensi dell'art. 7 della proposta di Regolamento, con il rappresentante designato dal prestatore di servizi o con un qualsiasi stabilimento dello stesso nell'ambito territoriale dell'Unione – essendo l'intervento dell'autorità competente del Paese di stabilimento meramente eventuale, e subordinato all'inottemperanza al provvedimento. Quest'ultimo, infatti, emesso o convalidato da un'autorità giudiziaria di uno Stato membro, è diretto, in assenza di intermediazioni, al *service provider*; a tale nozione si riconducono «i prestatori di servizi di comunicazione elettronica, i prestatori di servizi della società dell'informazione per i quali la conservazione dei dati è una componente propria del servizio fornito all'utente, compresi i *social network* nella misura in cui non possono essere considerati servizi di comunicazione elettronica, i mercati online che agevolano le operazioni tra utenti (come consumatori o imprese) e altri prestatori di servizi di *hosting*, e i prestatori di servizi di nomi di dominio internet e di numerazione»²³.

Significativa è la rilevanza attribuita ai sistemi di *cloud*, caratterizzati dal fatto che il *provider* non necessita di essere stabilito o di disporre di *server* in ogni giurisdizione, potendo invece avvalersi di un'amministrazione centralizzata e di sistemi decentrati per la prestazione dei servizi e l'accesso ai dati. Pertanto, si estende l'ambito di applicazione della proposta di Regolamento a «servizi *cloud* e altri servizi di *hosting* che forniscono una vasta gamma di risorse informatiche, quali reti, *server* o altre infrastrutture, mezzi di conservazione, *app* e servizi che permettono di conservare dati a diversi scopi»²⁴. Risultano invece escluse quelle attività nel cui ambito la conservazione dei dati rivesta un rilievo puramente accessorio, quali la prestazione di servizi giuridici, ingegneristici o contabili a distanza²⁵.

Si pongono in proposito, tuttavia, alcune questioni problematiche, sebbene la proposta valorizzi il ruolo dell'intervento dell'autorità giudiziaria in sede di emissione o convalida dell'or-

¹⁹ V. BELFIORE Rosanna (2015), p. 3288.

²⁰ Sulle ipotesi di mutuo riconoscimento "puro" contemplate dalla Direttiva in materia di OEI v. *ivi*, 3292-3293.

²¹ Cfr. CAMALDO Lucio (2014), "La direttiva sull'ordine europeo di indagine penale (OEI): un congegno di acquisizione della prova dotato di molteplici potenzialità, ma di non facile attuazione", *Diritto penale contemporaneo*.

²² V., sul tema, COLAIACOVO Guido (2017), pp. 169 ss.

²³ Proposta di Regolamento, cit., considerando n. 16. Secondo la definizione di cui all'art. 2, deve intendersi per *service provider* «la persona fisica o giuridica che fornisce una o più delle seguenti categorie di servizi: (a) servizi di comunicazione elettronica come definiti all'articolo 2, punto 4, della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche]; (b) servizi della società dell'informazione come definiti all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio⁴⁴, per i quali la conservazione dei dati è una componente propria del servizio fornito all'utente, tra cui i *social network*, i mercati online che agevolano le operazioni tra utenti e altri prestatori di servizi di *hosting*; (c) servizi di nomi di dominio internet e di numerazione IP, quali i prestatori di indirizzi IP, i registri di nomi di dominio, i registrar di nomi di dominio e i connessi servizi per la *privacy* o *proxy*».

²⁴ *Ivi*, considerando n. 16.

²⁵ *Ibidem*.

dine, che dovrebbe assicurare anche il rispetto dei principi di necessità e proporzionalità. Le criticità prospettabili sono connesse in particolare alla valutazione, ad opera del privato, di legittimità dell'ordine e della conseguente necessità di darvi effettivamente seguito. Invero, la proposta prevede ragioni di legittima opposizione all'esecuzione dell'ordine piuttosto circoscritte²⁶ - secondo una scelta da ritenersi opportuna in quanto consente, coerentemente peraltro con la logica propria del mutuo riconoscimento, il perseguimento di quegli obiettivi di celerità ed efficienza che rischierebbero, diversamente, di essere frustrati - ma al tempo stesso definite in termini non sempre specifici e pregnanti. Basti pensare, al riguardo, ai riferimenti alla manifesta violazione delle previsioni della Carta dei diritti fondamentali dell'Unione europea e alla manifesta arbitrarietà dell'ordine²⁷.

Non possono pertanto escludersi difficoltà applicative in capo ai privati destinatari dei provvedimenti, potenzialmente di ostacolo al raggiungimento degli stessi scopi di efficienza perseguiti, pur dovendosi considerare che la proposta di Direttiva in materia di *electronic evidence* dispone, come si vedrà, la designazione ad opera dei prestatori di servizi di soggetti i quali sarebbero specificamente preposti alla ricezione e all'esecuzione dei provvedimenti disciplinati dal Regolamento, e pertanto presumibilmente dotati di una certa competenza e specializzazione.

Un ulteriore correttivo è rappresentato dalla disposizione relativa all'intervento, nell'ipotesi di rifiuto da parte del destinatario di ottemperare al provvedimento, della competente autorità del Paese di esecuzione, la quale potrà valutare la sussistenza delle condizioni ostative individuate dal Regolamento, nonché far valere l'esistenza di interessi ulteriori, tipicamente statali, e individuati nell'operatività di un'immunità o di un privilegio ai sensi del proprio diritto interno, o l'incidenza della divulgazione dei dati su interessi fondamentali dello Stato, quali la sicurezza e la difesa nazionali. In caso di avvio da parte dell'autorità da ultimo indicata della procedura di esecuzione, le medesime ragioni di rifiuto potranno inoltre essere fatte valere dinanzi alla stessa²⁸.

4.2.

I destinatari degli ordini europei di produzione e di conservazione.

I destinatari dei provvedimenti sopra indicati - profilo specificamente oggetto della proposta di Direttiva - si individuano quindi nei rappresentanti legali appositamente designati dai prestatori di servizi per l'acquisizione delle prove; qualora questi non ottemperino, l'ordine dovrebbe essere trasmesso a un qualsiasi stabilimento del prestatore di servizi all'interno dell'U.E.²⁹, dovendo intendersi come tale, ai sensi dell'art. 2 della proposta, «l'esercizio effettivo di un'attività economica a tempo indeterminato con un'infrastruttura stabile a partire dalla quale viene svolta l'attività di prestazione di servizi, o l'infrastruttura stabile a partire dalla quale l'attività è gestita».

Le disposizioni proposte rispondono a una questione di particolare importanza nella materia considerata, quella dei diversi criteri utilizzati dagli Stati membri per l'affermazione della loro giurisdizione sui prestatori di servizi, e che possono consistere nel luogo di stabilimento,

²⁶ Secondo l'art. 14, par. 4, della proposta di Regolamento, «il destinatario può opporsi all'esecuzione dell'ordine europeo di produzione solo per uno dei seguenti motivi: (a) l'ordine europeo di produzione non è stato emesso o convalidato da un'autorità di emissione conformemente all'articolo 4; (b) l'ordine europeo di produzione non è stato emesso in relazione a un reato di cui all'articolo 5, paragrafo 4; (c) il destinatario non ha potuto ottemperare all'EPOC per impossibilità materiale o forza maggiore o perché l'EPOC contiene errori manifesti; (d) l'ordine europeo di produzione non riguarda dati conservati dal prestatore di servizi o per suo conto al momento della ricezione dell'EPOC; (e) il servizio esula dall'ambito di applicazione del presente regolamento; (f) dalle sole informazioni contenute nell'EPOC risulta che esso viola manifestamente la Carta dei diritti fondamentali dell'Unione europea o che è manifestamente arbitrario». Ai sensi del successivo par. 5, «il destinatario può opporsi all'esecuzione dell'ordine europeo di conservazione solo per i seguenti motivi: (a) l'ordine europeo di conservazione non è stato emesso o convalidato da un'autorità di emissione conformemente all'articolo 4; (b) il prestatore di servizi non ha potuto ottemperare all'EPOC-PR per impossibilità materiale o forza maggiore o perché l'EPOC-PR contiene errori manifesti; (c) l'ordine europeo di conservazione non riguarda dati conservati dal prestatore di servizi o per suo conto al momento della ricezione dell'EPOC-PR; (d) il servizio esula dall'ambito di applicazione del presente regolamento; (e) dalle sole informazioni contenute nell'EPOC-PR risulta che esso viola manifestamente la Carta dei diritti fondamentali dell'Unione europea o che è manifestamente arbitrario».

²⁷ A titolo esemplificativo, la Relazione illustrativa della proposta di Regolamento riconduce alla «manifesta arbitrarietà» l'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», in quanto lo stesso «ignorerebbe in modo manifesto le condizioni per l'emissione dell'ordine europeo di produzione previste dal regolamento e ciò sarebbe evidente già dal contenuto del certificato».

²⁸ V. par. 1, 2, 6, 7 del citato art. 14.

²⁹ Così dispone l'art. 7 della proposta di Regolamento.

in quello di prestazione del servizio o di ubicazione dei dati o in una combinazione degli stessi. Pertanto, l'introduzione di norme armonizzate che consentano alle competenti autorità dei diversi Paesi di conseguire gli elementi di prova digitali anche da un prestatore di servizi non rientrante nella loro giurisdizione, finanche stabilito all'esterno dell'UE, e di conoscere con certezza quale sia il soggetto a cui potere inoltrare l'ordine, appare particolarmente opportuna, in assenza, al momento, di un'auspicabile maggiore uniformità di criteri per la determinazione della giurisdizione degli Stati.

Lo stato di frammentazione giuridica esistente si ritiene invero pregiudizievole per gli stessi prestatori di servizi: «Attualmente gli Stati membri hanno approcci diversi per quanto riguarda gli obblighi imposti ai prestatori di servizi, specialmente nei procedimenti penali. La frammentazione riguarda soprattutto le prove elettroniche, dal momento che alcuni prestatori di servizi conservano informazioni che possono essere utili per l'indagine e il perseguimento di reati. Tale frammentazione crea incertezza giuridica per i soggetti coinvolti e può sottoporre i prestatori di servizi a obblighi e regimi sanzionatori differenti e talvolta in conflitto tra loro a tale riguardo, a seconda del fatto che forniscano i loro servizi a livello nazionale, a livello transnazionale all'interno dell'Unione o al di fuori dell'Unione. Per ridurre gli ostacoli alla libera prestazione di servizi, la direttiva rende obbligatorio per i prestatori di servizi designare un rappresentante legale nell'Unione incaricato di ricevere decisioni volte ad acquisire prove emesse dalle autorità nazionali competenti nei procedimenti penali, ottemperare a tali decisioni e farle eseguire. La riduzione degli ostacoli che ne conseguirebbe migliorerebbe il funzionamento del mercato interno in modo coerente con lo sviluppo di uno spazio comune di libertà, sicurezza e giustizia»³⁰.

Si deve comunque precisare che la proposta Direttiva si configura quale applicabile ai prestatori di servizi i quali non si limitino a rendere fruibile il servizio all'interno dell'Unione, bensì abbiano un "collegamento sostanziale" con quest'ultima, da intendersi come disponibilità di uno stabilimento all'interno dell'Unione stessa, o di un numero significativo di utenti in uno o più Stati membri, o come orientamento dell'attività verso uno o più Stati membri, desumibile da una varietà di elementi tra loro eterogenei, che vanno dall'uso della lingua o della moneta dello Stato, alla disponibilità di una "app" nell'"app store" nazionale, alla pubblicità locale, alla gestione dei rapporti con la clientela. Precisa la Relazione illustrativa che «il criterio del collegamento sostanziale dovrebbe inoltre considerarsi soddisfatto qualora il prestatore di servizi diriga le sue attività verso uno o più Stati membri, come previsto all'articolo 17, paragrafo 1, lettera c), del regolamento (UE) n. 1215/2012 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale»³¹.

L'obbligo di nomina del rappresentante in uno Stato membro in cui il service provider sia stabilito o preli servizi è volto ad evitare scelte "strategiche" del Paese di riferimento, in base, ad esempio, alle sanzioni previste in caso di inottemperanza al provvedimento conseguente all'esperimento della procedura di esecuzione.

Significativa è altresì la presa d'atto³² dell'esistenza di servizi quali quelli di *hosting* o *software*, tali da comportare la conservazione dei dati all'interno di un'infrastruttura affidata dal *provider* a una diversa società. In tal caso, salvo che sia inopportuno procedere secondo tale modalità per ragioni di potenziale compromissione delle indagini, l'accesso alla prova elettronica dovrebbe intervenire mediante il coinvolgimento della società stessa. Potranno tuttavia trovare applicazione, in questo caso, strumenti diversi rispetto a quelli oggetto del Regolamento – quali, a titolo esemplificativo, l'ordine europeo di indagine – essendo gli ordini europei di produzione e conservazione riservati ai soggetti qualificabili come "prestatori di servizi".

La designazione di soggetti specificamente preposti alla gestione degli ordini di trasmissione o conservazione di elementi che rivestano rilievo probatorio in procedimenti penali può ritenersi apprezzabile, in quanto tale da agevolare – secondo gli auspici degli stessi redattori della proposta normativa – le autorità competenti nell'individuazione dei destinatari dei provvedimenti emessi, coerentemente con la rapidità che deve contraddistinguere le indagini implicanti l'accesso all'*electronic evidence*, e da arginare le difficoltà incontrate dagli stessi prestatori di servizi nella risposta alle richieste ricevute, invero sempre più frequenti³³.

L'obbligo posto in capo ai prestatori di servizi all'interno dell'Unione di designare rappre-

³⁰ Così la Relazione illustrativa della proposta.

³¹ *Ivi*, 9.

³² V. in tal senso l'art. 5 della medesima proposta.

³³ V. la Relazione illustrativa della citata proposta di Direttiva.

sentanti è peraltro già previsto da alcune norme in particolari settori, tra cui il Regolamento generale sulla protezione dei dati personali 2016/679³⁴ e la Direttiva (UE) 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione³⁵.

Con riguardo al modello del contatto diretto con i privati prestatori di servizi, deve altresì ricordarsi come, pur rivestendo la cooperazione con tali soggetti, nel diverso contesto del Consiglio d'Europa, una rilevanza particolare ai sensi delle previsioni della Convenzione di Budapest sulla criminalità informatica del 2001, non sia ancora contemplata espressamente l'ipotesi di un contatto diretto con il privato stabilito al di fuori della giurisdizione dello Stato procedente. Proprio nella direzione da ultimo indicata, come si dirà, va quindi il progetto di secondo protocollo addizionale alla Convenzione; nondimeno, si è rilevato come nella prassi non siano infrequenti le richieste di fornitura di dati e informazioni rivolte da uno Stato al privato straniero, e rimesse alla volontaria scelta di collaborazione di quest'ultimo. Si registra, in particolare, una significativa tendenza dei *service providers* stabiliti negli Stati Uniti e in Irlanda a fornire spontaneamente alle autorità di altri Paesi gli elementi di rilievo probatorio³⁶, seppure a certe condizioni quali il fatto che, negli U.S.A., non si tratti di dati relativi al "contenuto".

4.3. *I tempi delle procedure.*

Una delle ragioni principali che si sono poste alla base della proposta in esame è rappresentata dalla riduzione dei tempi legati allo svolgimento di procedure pur "agili", quali quella dell'ordine europeo di indagine. In relazione a quest'ultimo, invero, in via generale la decisione sul riconoscimento e l'esecuzione dell'ordine deve essere adottata dall'autorità di esecuzione entro trenta giorni dalla ricezione dell'OEI, e l'esecuzione stessa deve avere luogo «senza ritardo», e comunque nel termine di novanta giorni dalla decisione stessa, salve le eccezioni contemplate dalla norma, nonché le proroghe ammesse per particolari motivi³⁷.

Significativamente più contenuti appaiono invece i tempi legati all'esecuzione degli ordini di produzione e conservazione, fissati dall'art. 9 della proposta di Regolamento in dieci giorni, riducibili fino a sei ore nei casi di urgenza.

4.4. *Profili attinenti alla tutela dei diritti.*

Analogamente a quanto previsto in materia di ordine europeo di indagine³⁸, si subordina l'operatività dei nuovi strumenti al rispetto dei principi di necessità e di proporzionalità.

Può sul punto ricordarsi che la normativa di attuazione delle disposizioni europee in materia di OEI, in tal senso discostandosi dall'orientamento della giurisprudenza di Strasburgo, che rimette alle autorità nazionali il bilanciamento tra i diversi interessi che entrano in gioco

³⁴ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), art. 27.

³⁵ Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione; il relativo art. 18 prevede che il prestatore di servizi digitali non stabilito nell'U.E., ma che presti servizi al suo interno, si consideri stabilito nello Stato membro nel cui ambito ha designato il proprio rappresentante.

³⁶ ALLEGREZZA Silvia (2018), p.150.

³⁷ Secondo la normativa in materia di ordine europeo di indagine (v. in particolare l'art. 12 della citata Direttiva 2014/41/UE), l'autorità di emissione può comunque rappresentare a quella di esecuzione l'esistenza di circostanze, legate a termini procedurali, gravità del reato o «altre circostanze particolarmente urgenti», che rendono necessario svolgere le attività considerate in tempi più rapidi, o eseguire l'OEI in una determinata data.

³⁸ L'art. 6 della citata Direttiva 2014/41/UE subordina l'emissione dell'ordine a una valutazione di necessità e di proporzionalità dello stesso, tenuto conto dei diritti dei soggetti sottoposti a procedimento. Il considerando n. 11 riferisce inoltre la valutazione di proporzionalità, al pari di quella di necessità, tanto alla prova, quanto all'atto di indagine funzionale all'acquisizione degli elementi di prova, quanto, ancora, all'emissione di un OEI al fine di conseguire la partecipazione di un altro Stato al medesimo atto, precisando altresì che l'autorità di esecuzione dovrebbe disporre della facoltà di porre in essere un atto meno intrusivo di quello richiesto, qualora esso consenta di conseguire risultati analoghi. Parte della dottrina ha espresso un orientamento critico rispetto alla prevista possibilità che l'autorità di esecuzione operi un'inedita consultazione dell'autorità di emissione, quando ritenga non rispettato il requisito di proporzionalità, in quanto si è osservato che tale vaglio è tale da introdurre, di fatto, nuove ipotesi di rifiuto, in contrasto con l'ispirazione della normativa in considerazione al principio del mutuo riconoscimento: in questo senso BELFIORE Rosanna (2015), pp. 3292-3293.

quando sia necessario compiere una determinata attività investigativa, specifica i criteri secondo cui la valutazione di proporzionalità deve operare³⁹. Essi attengono, in particolare, ai sensi dell'art. 8 d.lgs. 108/2017, alla possibilità di ritenere giustificato il sacrificio dei diritti dell'imputato, o della persona sottoposta alle indagini o comunque coinvolta dal compimento dell'atto richiesto, alla luce delle esigenze investigative e probatorie del caso concreto, tenuto conto della gravità del reato per cui si procede e della pena per lo stesso stabilita. Si potrebbe quindi immaginare, in proposito, un riferimento, quantomeno indicativo, a tali criteri anche ai fini della valutazione di necessità e proporzionalità dei nuovi provvedimenti proposti; la considerazione della gravità dell'illecito, nella valutazione di proporzionalità operata dall'autorità di emissione, è peraltro menzionata nella Relazione illustrativa della proposta di Regolamento.

Se, inoltre, in via generale, la normativa in materia di OEI sancisce la necessità di assicurare protezione ai diritti della persona sottoposta a procedimento, richiedendo altresì la tutela dei principi fondamentali dell'ordinamento giuridico dello Stato di esecuzione e imponendo il rispetto dei diritti difensivi e dei principi del giusto processo nell'ambito del processo celebrato nello Stato di emissione⁴⁰, la proposta in esame ribadisce l'operatività dei principi stessi, riconoscendo una primaria rilevanza, in ragione del suo più ristretto ambito di applicazione, alla salvaguardia della riservatezza dei dati.

Emerge quindi confermata la centralità nel diritto europeo del principio di proporzionalità: secondo quanto si è osservato, «la vera cifra che caratterizza quest'ultimo e che disegna una diversa concezione di legalità a forte componente "giudiziale" è infatti rappresentata da quel bilanciamento di valori e da quelle modulazioni applicative che si esprimono in modo precipuo nel canone di proporzionalità»⁴¹.

Si premette comunque la potenziale incidenza dei provvedimenti oggetto delle norme citate su una pluralità di situazioni soggettive facenti capo ai diversi soggetti coinvolti: «diritti delle persone fisiche ai cui dati è previsto l'accesso: il diritto alla protezione dei dati personali; il diritto al rispetto della vita privata e familiare; il diritto alla libertà di espressione; il diritto alla difesa; il diritto a un ricorso effettivo e a un giudice imparziale; i diritti del prestatore di servizi: il diritto alla libertà d'impresa; il diritto a un ricorso effettivo; i diritti di tutti i cittadini: il diritto alla libertà e alla sicurezza»⁴². Analogamente a quanto previsto in relazione all'OEI, la proposta sancisce, in via generale, l'esigenza di rispetto dei principi fondamentali in materia penale e di processo penale, quali il diritto ad un equo processo, garantito dall'art. 6 CEDU e dagli artt. 47 e 48 della Carta dei diritti fondamentali dell'Unione europea; torna inoltre il rinvio alle direttive europee in materia di garanzie difensive, comune ad altri strumenti di cooperazione in ambito europeo⁴³.

Significativa è altresì la valorizzazione delle esigenze di tutela della libertà di prestazione di servizi dei soggetti i quali svolgano attività implicanti, quale aspetto non secondario, la conservazione dei dati che rendano possibile risalire all'identità dell'utente, ovvero alle caratteristiche "estrinseche" o di contenuto delle operazioni; l'attenzione prestata a tali istanze si riflette par-

³⁹ Trogu Mauro (2018), p. 1030. Cfr., nel senso dell'auspicio di una certa «tipizzazione» di determinati modelli di bilanciamento ad opera della Corte di giustizia, Kostoris Roberto E. (2018), p. 1448. L'Autore pone in luce la centralità del principio di proporzionalità, in quanto tale da consentire, pur in un contesto «fluido» quale quello europeo, un rilevante strumento di controllo dell'operato del giudice.

⁴⁰ V. l'art. 15 della Direttiva 2014/41/UE. Il rispetto dei principi fondamentali dell'ordinamento dello Stato di esecuzione rappresenta un correttivo al criterio della *lex loci*: cfr. Camaldo Lucio (2014). In materia di squadre investigative comuni, si è rilevato come il criterio della *lex loci*, sancito dall'art. 1, par. 3, lett. b) della decisione quadro, sia temperato dalle previsioni che subordinano l'utilizzabilità dell'atto investigativo compiuto all'estero al rispetto delle regole processuali proprie dell'ordinamento giuridico ospitante, consentendo di salvaguardare le esigenze legate al rispetto dei diritti dei soggetti sottoposti a procedimento penale. Con riferimento, infine, alla Procura europea, si può evidenziare come, secondo le previsioni del Regolamento istitutivo, l'applicazione delle normative nazionali intervenga in relazione a tutti quegli aspetti che non siano disciplinati dall'atto europeo, e come una rilevanza centrale rivesta la struttura "decentrata" del medesimo organo, operante per lo più attraverso i procuratori delegati titolari delle indagini relative a fatti commessi nell'ambito del loro territorio, implicanti il compimento di atti che si svolgeranno essenzialmente secondo le regole proprie dello Stato di riferimento. Il criterio della possibilità di adottare il provvedimento in una situazione interna analoga nello Stato di emissione è sancito anche dall'art. 5 della proposta di Regolamento.

⁴¹ Kostoris Roberto E. (2018), p. 1448.

⁴² V. la Relazione illustrativa della proposta di Regolamento.

⁴³ Si tratta, in particolare, della Direttiva 2010/64/UE sul diritto all'interpretazione e alla traduzione nei procedimenti penali, della Direttiva 2012/13/UE sul diritto a ricevere informazioni relative ai diritti e all'accusa e ad accedere al fascicolo, della Direttiva 2013/48/UE relativa al diritto di avvalersi di un difensore e di comunicare con familiari al momento dell'arresto e della detenzione, della Direttiva 2016/343 sul rafforzamento di alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo, della Direttiva 2016/800 sulle garanzie procedurali per i minori e la direttiva 2016/1919 sull'ammissione al patrocinio a spese dello Stato per indagati e imputati nell'ambito di procedimenti penali e per le persone ricercate nell'ambito di procedimenti di esecuzione del mandato d'arresto europeo. Si può ricordare come, salvo il riferimento nella normativa in materia di OEI ai principi e ai diritti fondamentali che si sono indicati, anche le disposizioni in materia di Procura europea operino un rinvio alle tutele riconducibili alla Carta dei diritti fondamentali dell'UE, alle direttive citate, nonché alle garanzie poste dagli ordinamenti nazionali.

ticularmente nella proposta di Direttiva, volta espressamente, tra l'altro, a delineare un quadro normativo chiaro e uniforme in materia di obblighi di cooperazione dei *service providers*, e di modalità di ottemperanza ai relativi ordini giudiziari.

Venendo quindi al profilo centrale della riservatezza dei dati oggetto degli ordini di produzione e conservazione, l'art. 2 della proposta di Regolamento, coerentemente con quanto previsto negli ordinamenti di numerosi Stati membri, opera una distinzione tra gli stessi sulla base della loro eventuale attinenza al "contenuto"; più specificamente, si individuano, quali categorie di informazioni suscettibili di acquisizione a scopo probatorio, i dati relativi agli accessi⁴⁴, alle operazioni⁴⁵ e al contenuto⁴⁶, sebbene sia espressamente ricordato come esse ricadano, senza distinzioni, nell'ambito di applicazione della normativa europea in materia di tutela dei dati personali⁴⁷.

Può essere interessante rilevare come la stessa proposta dia atto della rilevanza della differenziazione delle categorie di informazioni di cui sopra anche in ordinamenti esterni all'Unione: ne costituisce un esempio quello statunitense, la cui normativa in materia consente ai *service providers* di condividere su base volontaria con le autorità di contrasto straniere i dati che non siano relativi al contenuto, salve limitate eccezioni⁴⁸.

Pertanto, in considerazione della diversa incidenza dei provvedimenti concernenti le varie categorie di dati sui diritti alla riservatezza, al rispetto della vita privata e familiare, alla libertà di espressione dei relativi titolari, si prevede, all'art. 5, che l'ordine europeo di produzione possa essere emesso per qualsiasi reato se concernente i dati relativi agli accessi e agli abbonati, e sia invece riservato all'accertamento di crimini di maggiore gravità, per cui la legge preveda la pena della reclusione superiore nel massimo a tre anni, o che rientrino nella categorie individuate dalla medesima disposizione, se riguardante i dati relativi al contenuto⁴⁹. L'ordine europeo di conservazione può operare indipendentemente da limiti di gravità del reato per cui si procede; la mancata previsione di requisiti di tal genere rispetto a questa ipotesi, nonché, come detto, all'ordine di produzione che concerna dati relativi agli accessi e agli abbonati è stata oggetto di critica, in quanto, al pari dei presupposti di necessità e di proporzionalità, tale da comportare il rischio di un abuso di strumenti altamente "intrusivi" ad opera delle autorità di contrasto⁵⁰.

Secondo quanto espressamente indicato nella proposta di Regolamento⁵¹, le relative prescrizioni si estendono anche ai dati criptati, analogamente a quanto è prescritto in tema di "ordine europeo di intercettazione". Evidente è la rilevanza di tali previsioni quando vengano in considerazione applicazioni, quali *Whatsapp* o *Skype*, che utilizzino tecniche di questo genere al fine di ostacolare l'accesso ai dati.

Il problema dell'interferenza tra le esigenze proprie dell'attività di accertamento di fatti penalmente illeciti e la tutela da assicurare ai diritti fondamentali dei soggetti coinvolti, tra cui la riservatezza dei dati conservati dal *service provider*, è emerso, in tempi piuttosto recenti, nel noto caso – seppure non implicante un accesso alla prova digitale di natura transfrontaliera – relativo alla richiesta rivolta ad Apple dall'Fbi nell'ambito delle investigazioni successive all'attentato terroristico di San Bernardino del dicembre 2015⁵². Come è noto, la società

⁴⁴ Si tratta dei dati, «tipicamente (...) registrati nell'ambito di una registrazione di eventi (in altre parole un *log server*) per indicare l'inizio e la fine di una sessione di accesso utente a un servizio», che consentono di risalire all'identità dell'utente – eventualmente a seguito dell'acquisizione dei dati relativi agli abbonati – per il tramite di un indirizzo IP o di altro identificatore che individui l'interfaccia di rete utilizzata per l'accesso (v. considerando n. 21 della proposta; per la relativa definizione, cfr. l'art. 2). A tali informazioni sono accostati, sotto il profilo del livello di incidenza sui diritti fondamentali, i dati relativi agli abbonati.

⁴⁵ Si tratta dei dati che rendono possibile risalire ai contatti dell'utente e al luogo in cui questo si trova (v. considerando n. 22 della proposta di Regolamento e, ancora, per la relativa definizione, il citato art. 2).

⁴⁶ L'art. 2 della proposta di Regolamento li identifica con «qualsiasi dato conservato in formato digitale, come testo, voce, video, immagine o suono, diverso dai dati relativi agli abbonati, agli accessi e alle operazioni».

⁴⁷ V. la proposta di Regolamento, cit., considerando n. 23.

⁴⁸ V., sul punto, il considerando n. 19 della proposta di Regolamento.

⁴⁹ Questi ultimi, come espressamente chiarito, sono «reati armonizzati» la cui prova è tipicamente disponibile solo in formato elettronico: i) la decisione quadro 2001/413/GAI del Consiglio relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, ii) la direttiva 2011/92/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio e iii) la direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio. L'ordine può essere emesso anche per i reati elencati nella direttiva (UE) 2017/541 sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio.

⁵⁰ GIALUZ Mitja, DELLA TORRE Jacopo (2018), p. 293.

⁵¹ Secondo il considerando n. 19 della proposta, i dati devono essere forniti indipendentemente dal fatto che siano criptati o meno.

⁵² V. SIGNORATO Silvia (2016), p. 198.

produttrice dell'*iPhone* ha rifiutato l'accoglimento della richiesta diretta alla modifica di una caratteristica propria del dispositivo, e tale da implicare la distruzione dei dati ivi contenuti a seguito di un certo numero di tentativi infruttuosi di inserimento del codice di blocco, sebbene in seguito gli investigatori siano riusciti comunque ad accedere alle informazioni archiviate nello *smartphone* interessato⁵³.

Sotto il diverso profilo della garanzia del diritto di difesa della persona a cui si riferiscono i dati acquisiti, l'art. 11 della proposta di Regolamento contiene previsioni espressamente⁵⁴ tese a contemperare le esigenze di salvaguardia dell'attività di indagine con quelle connesse alla tutela della riservatezza dei soggetti coinvolti dall'accesso ai dati, e che dovranno essere informati, se non dallo stesso *service provider*, comunque dall'autorità di emissione, quando non vi sia più pericolo di pregiudizio per le investigazioni, in conformità con l'art. 13 della Direttiva sulla protezione dei dati nelle attività di polizia e giustizia. Si prescrive in particolare, nella prospettiva dell'utile esperimento dei mezzi di impugnazione, l'informativa sui mezzi di ricorso disponibili. Le disposizioni di cui all'art. 11 della proposta in esame si ispirano, per espressa indicazione dei redattori⁵⁵, all'art. 19 della Direttiva in materia di ordine europeo di indagine. Quest'ultimo deve essere considerato congiuntamente al considerando n. 22 della medesima Direttiva 2014/41/UE, secondo cui lo Stato di esecuzione dovrebbe garantire mezzi di impugnazione almeno equivalenti a quelli previsti per atti interni analoghi⁵⁶.

Proseguendo nella trattazione di alcune delle questioni che possono ritenersi più significative sul piano del bilanciamento tra esigenze di effettività dell'attività investigativa e tutela dei diritti fondamentali, con riguardo ai provvedimenti di cui si propone l'introduzione, merita particolare attenzione la già rilevata⁵⁷ possibilità che gli ordini siano diretti a rappresentanti di *providers* che, pur prestando i propri servizi all'interno dell'Unione, siano stabiliti in Paesi terzi, i cui ordinamenti garantiscano un più elevato livello di tutela della riservatezza o di altri diritti fondamentali. Basti pensare al caso degli Stati Uniti, il cui *Electronic Communications Privacy Act (EPA)* vieta la divulgazione di dati relativi al contenuto, rientranti nell'ambito geografico di applicazione dello stesso, fatta eccezione per ipotesi limitate. Premesso che la questione dei rapporti con i *service providers* statunitensi sarà oggetto di apposita trattazione, si deve rilevare come il problema sia stato considerato dalle proposte normative in esame, le quali contemplano la possibilità che il destinatario dell'ordine di produzione, qualora ritenga l'ottemperanza allo stesso in contrasto con il diritto applicabile di un Paese terzo che vieti la divulgazione dei dati per motivi diversi da quelli di cui all'articolo 15, informi l'autorità di emissione dei motivi per non eseguire l'ordine conformemente alla procedura di cui all'art. 9, par. 5.

4.5. *I mezzi di impugnazione.*

La proposta di Regolamento elaborata dalla Commissione europea pone previsioni diverse in materia di impugnazioni, in relazione ai soggetti coinvolti dai provvedimenti adottati.

Per quanto concerne i prestatori di servizi, si può rinviare a quanto si è detto in precedenza in materia di opposizione all'ordine emesso dall'autorità straniera, con la precisazione per cui, qualora l'autorità dello Stato di esecuzione decida di dare corso all'ordine pur a fronte delle deduzioni del destinatario, è fatto salvo il diritto a un ricorso giurisdizionale nei confronti del provvedimento dell'autorità dello Stato di esecuzione.

In capo ai soggetti titolari dei dati, invece, l'art. 17 della proposta di Regolamento pone il diritto a un ricorso giurisdizionale nello Stato di emissione, seppure limitatamente all'ordine europeo di produzione, che è l'unico a comportare la divulgazione effettiva dei dati stessi. In senso critico rispetto a tale previsione si sono espressi peraltro i primi commentatori delle

⁵³ *Ibidem*.

⁵⁴ Cfr. la Relazione illustrativa, 21.

⁵⁵ *Ibidem*.

⁵⁶ Gli artt. 4 e 13 d.lgs. 108/2017 prevedono che nel nostro ordinamento il decreto di riconoscimento sia comunicato al difensore nel termine stabilito per l'avviso di cui ha diritto secondo la legge italiana; qualora le norme processuali stabiliscano il diritto all'assistenza all'atto di indagine, ma non al previo avviso, la comunicazione interviene contestualmente al compimento dell'atto stesso o subito dopo. L'impugnazione avverso il decreto di riconoscimento dell'ordine, che assume la forma dell'opposizione al g.i.p. del tribunale presso cui ha sede la procura della Repubblica che ha provveduto al riconoscimento, è ammessa entro cinque giorni dalla comunicazione: cfr. Trogu Mauro (2018), pp.1020 ss. e 1046 ss.

⁵⁷ V. *supra*, par. 4.1.

proposte normative in esame, i quali, ritenendo le stesse sbilanciate nella direzione del soddisfacimento delle esigenze repressive, più che in quella della tutela dei diritti fondamentali, hanno rilevato che anche la semplice indisponibilità di determinati dati che si riferiscono alla propria persona per un certo periodo di tempo è tale da tradursi in una limitazione di libertà tale da richiedere quantomeno la previsione di mezzi di impugnazione adeguati⁵⁸.

Sono comunque fatti salvi gli strumenti di ricorso previsti dagli atti normativi dell'Unione in materia di tutela dei dati personali. Si precisa altresì che «i termini o altre condizioni per la proposizione del ricorso sono uguali a quelli previsti in casi interni analoghi e sono applicati in modo da garantire alle persone interessate l'esercizio effettivo del ricorso»⁵⁹.

L'art. 17 della proposta specifica che il gravame dovrebbe essere proposto da indagati e imputati all'interno del procedimento penale, e dagli altri soggetti interessati avvalendosi degli strumenti previsti nello Stato di emissione. Sul punto, può rilevarsi come le previsioni considerate siano molto generali – e lo siano comprensibilmente, se si ha riguardo alle differenze normative rinvenibili in materia tra gli Stati membri – ma al tempo stesso possano implicare qualche difficoltà nell'individuazione dei mezzi di impugnazione esperibili nell'ordinamento interno, attesa la diretta applicabilità delle disposizioni del Regolamento.

Si potrebbe quindi ipotizzare, anche in questo caso, il riferimento a quanto stabilito dalla nostra legge processuale rispetto a casi interni analoghi, ossia alle previsioni in materia di impugnazione del provvedimento di sequestro probatorio di dati relativi a sistemi informatici o telematici, *ex artt. 254-bis e 257 c.p.p.*, nell'ambito del procedimento penale aperto nello Stato di emissione.

Giova ricordare, sul punto, che la normativa di attuazione della Direttiva in materia di OEI, a fronte della disposizione di cui all'art. 14 relativa alla necessità che siano previsti mezzi d'impugnazione equivalenti a quelli disponibili in un caso interno analogo, all'art. 13 d.lgs. 108/2017 ha disciplinato un apposito strumento di contestazione anche del decreto di riconoscimento dell'ordine, consistente nell'opposizione al giudice per le indagini preliminari. La medesima Direttiva ha invece limitato la contestazione del provvedimento per motivi di merito all'esperimento di un'azione nello Stato di emissione dell'OEI.

5. La cooperazione con i *service providers* stabiliti in Stati terzi: il caso degli Stati Uniti.

Come si è avuto modo di osservare, le stesse proposte normative esaminate, pur introducendo le previsioni in materia di nomina di rappresentanti ad opera dei *providers* che forniscono il proprio servizio all'interno dell'U.E., prendono atto delle criticità riconducibili all'esigenza di accedere a dati detenuti da soggetti stabiliti in Paesi terzi, attese le possibili differenze normative riscontrabili tra gli ordinamenti di questi ultimi e quelli degli Stati membri, anche sotto il profilo della tutela della riservatezza e degli altri diritti fondamentali.

Si è già evidenziato il caso degli Stati Uniti, in cui la trasmissione dei dati relativi al "contenuto" è soggetta a limiti rigorosi. Nondimeno, si può anche osservare come proprio in tale Paese abbiano sede molti dei più importanti *Internet providers*: basti pensare a Facebook, Google, Twitter.

La possibilità di accesso ai dati detenuti da tali soggetti, ad opera delle autorità degli Stati membri dell'Unione, è stata in passato assicurata dal *Mutual Legal Assistance Agreement* stipulato tra U.S.A. e U.E., sebbene i tempi particolarmente significativi connessi allo svolgimento delle procedure di mutua assistenza si siano rivelati sovente incompatibili con le esigenze legate all'acquisizione di elementi probatori caratterizzati da estrema volatilità e suscettibili di modifica e alterazione. Pertanto, in sede di revisione dell'accordo, nel 2016, gli Stati membri erano stati incoraggiati a porre in essere contatti diretti con i *providers* statunitensi, al fine di conseguire gli obiettivi di accesso alla prova digitale. La collaborazione volontaria dei prestatori di servizi digitali era quindi andata configurandosi quale alternativa alla cooperazione giudiziaria tra le autorità competenti dei Paesi coinvolti, sebbene il carattere non doveroso della prima avesse determinato una gestione delle richieste ad opera dei relativi destinatari secondo un approccio casistico, o fondato su criteri dagli stessi autonomamente determinati.

⁵⁸ GIALUZ Mitja, DELLA TORRE Jacopo (2018), p. 292.

⁵⁹ V. l'art. 17 della proposta di Regolamento.

Si può pensare, a tale ultimo proposito, alle linee guida elaborate da Facebook, Apple, Google⁶⁰.

Proprio le criticità sopra menzionate hanno quindi condotto la Commissione, nel febbraio 2019, a proporre due mandati negoziali, soggetti all'approvazione del Consiglio; essi concernono l'uno i rapporti con gli Stati Uniti, l'altro la partecipazione ai negoziati relativi al secondo Protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica, a cui si è fatto cenno e di cui si tratterà più ampiamente nel prossimo paragrafo⁶¹.

Con riguardo all'auspicato accordo con gli Stati Uniti, esso tende alla creazione di regole comuni, tali da assicurare il superamento degli ostacoli alla cooperazione in materia di accesso alla *digital evidence* riconducibili alle differenze normative tra i Paesi interessati, nonché la sicurezza dei dati trasferiti e un elevato livello di tutela dei diritti fondamentali, coerentemente con la Carta dei diritti fondamentali dell'Unione europea, i principi generali del diritto dell'Unione e la giurisprudenza della Corte di giustizia⁶². Tali nuove disposizioni, nelle intenzioni della Commissione europea, dovrebbero costituire il completamento dell'*EU-U.S. Data Protection and Privacy Agreement*, stipulato nel 2017, nonché lo *U.S. Judicial Redress Act*.

Si pone infine in evidenza come la proposta di avvio di negoziati da parte della stessa Unione europea sia volta proprio a evitare la riproposizione di quella frammentazione normativa che deriverebbe dalla conclusione di singoli accordi bilaterali tra gli Stati Uniti, i diversi Stati membri dell'U.E. e Paesi terzi⁶³.

6. Il progetto di un secondo protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica: cenni.

Si è appena avuto modo di osservare come la Commissione europea abbia proposto l'avvio di negoziati anche per il coinvolgimento dell'Unione europea nella stipula del secondo protocollo addizionale alla Convenzione di Budapest del 2001, ancora allo stadio di progetto normativo.

Invero, le nuove sfide ed esigenze legate all'accesso transfrontaliero all'*electronic evidence* hanno condotto gli Stati membri del Consiglio d'Europa a ricercare soluzioni, prima attraverso un apposito gruppo di lavoro operante dal 2012 al 2014, e poi, dal 2015 al 2017, per il tramite del *Cloud Evidence Group*⁶⁴.

Si può notare come gli obiettivi perseguiti mediante il progetto normativo in esame siano del tutto analoghi a quelli che ispirano le proposte recentemente sviluppate dalla Commissione europea: vengono in particolare in considerazione le esigenze di incremento della rapidità e dell'efficienza della cooperazione in materia di accesso alla prova digitale, da perseguire anche mediante l'instaurazione di forme dirette di contatto tra le autorità competenti dei Paesi che abbiano sottoscritto la Convenzione e il *service provider* stabilito in altro Stato parte.

Deve peraltro ricordarsi come la previsione di obblighi di collaborazione in capo ai prestatori di servizi, ma limitatamente a quelli rientranti nell'ambito della giurisdizione propria dello Stato precedente, era già una caratteristica propria della Convenzione, come testimoniano alcune norme del nostro ordinamento processuale, e in particolare quelle in materia di sequestro probatorio di cui all'art. 254-bis c.p.p.

⁶⁰ Si considerino, a titolo esemplificativo, i criteri predisposti da Facebook: «*With regard to requests from:- USA authorities, Facebook "disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act ("SCA"), 18 U.S.C. Sections 2701-2712."* - *International requests, Facebook "disclose account records solely in accordance with our terms of service and applicable law. A Mutual Legal Assistance Treaty request or letter rogatory may be required to compel the disclosure of the contents of an account."*

*Facebook Ireland Limited is a subsidiary of Facebook Inc. All users outside of the USA and Canada apparently have a contract with Facebook Ireland Limited. Under its "data policy", Facebook may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards» (v. CYBERCRIME CONVENTION COMMITTEE (T-CY), *Criminal justice access to data in the cloud: Cooperation with "foreign" service providers*, 3 maggio 2016.*

⁶¹ COMMISSIONE EUROPEA, *Security Union: Commission recommends negotiating international rules for obtaining electronic evidence*, in www.europa.eu, 5 febbraio 2019.

⁶² COMMISSIONE EUROPEA, *Questions and Answers: Mandate for the EU-U.S. cooperation on electronic evidence*, in www.europa.eu, 5 febbraio 2019.

⁶³ *Ibidem*.

⁶⁴ COUNCIL OF EUROPE, *Enhanced international cooperation on cybercrime and electronic evidence: Towards a Protocol to the Budapest Convention*, in www.rm.coe.int, 19 marzo 2018.

7.

Considerazioni conclusive.

In conclusione, può dirsi oggetto di una crescente attenzione, non solo nell'ambito dell'Unione europea, un nuovo modello di cooperazione tra gli Stati per l'acquisizione degli elementi di prova in formato elettronico, quello del contatto diretto tra le autorità che procedano per un determinato illecito e il prestatore di servizi – o il suo rappresentante o stabilimento – il quale detenga i dati al di fuori dell'ambito territoriale del Paese procedente.

I benefici in termini di rapidità ed efficienza che possono derivarne alle indagini sono senza dubbio apprezzabili, così come merita di essere considerato favorevolmente il tentativo di individuare una soluzione effettiva ad uno dei problemi più significativi della materia, costituito dai rapporti con Paesi terzi, le cui normative interne possono costituire un ostacolo alla messa a disposizione dei dati. Esigenze di uniformità delle disposizioni applicabili e di comparabilità dei rispettivi livelli di tutela dei diritti fondamentali si pongono in maniera sempre più pressante, e può ritenersi pertanto auspicabile la prosecuzione dell'Unione europea nel percorso che la avvicina, dopo alcuni sviluppi particolarmente significativi conosciuti dalla cooperazione giudiziaria in materia penale, e in conformità con il principio del mutuo riconoscimento, a un modello innovativo di svolgimento dell'attività investigativa oltre i confini nazionali.

Si rivela peraltro apprezzabile l'intento di coniugare le istanze relative all'efficacia dell'attività di raccolta degli elementi di prova con la garanzia di un elevato livello di tutela dei diritti fondamentali dei soggetti i quali siano, a vario titolo, dalla stessa coinvolti, sebbene non manchino alcuni elementi di criticità, secondo quanto si è avuto modo di osservare.

Le proposte normative considerate necessitano indubbiamente di chiarificazione, sotto alcuni profili, essendo ravvisabili taluni aspetti problematici, e potenzialmente fonti di incertezze, delle medesime – quali, a titolo esemplificativo, le previsioni concernenti la contestazione degli ordini e i mezzi di impugnazione – e persistendo il significativo ostacolo legato alle differenze normative rinvenibili tra i diversi Paesi, in merito a profili essenziali quali la stessa determinazione dell'assoggettamento di un determinato *provider* alla giurisdizione statale.

Il problema della disomogenea definizione dei criteri di attribuzione della giurisdizione, con il rischio di avvio di procedimenti in una pluralità di Paesi, continua ad essere di particolare serietà, in particolare in materia di reati informatici, anche in ragione – secondo quanto si è osservato – della scarsa adeguatezza, rispetto alle indagini informatiche, di previsioni quali quelle del nostro codice penale, che legano la potestà punitiva statale⁶⁵ alla commissione del fatto entro il territorio dello stesso, salvi i casi di procedibilità per illeciti commessi all'estero. Si è peraltro osservato⁶⁶ come la legge 18 marzo 2008, n. 48 non abbia recepito la norma di cui all'art. 22, par. 5, della Convenzione di Budapest, che ha previsto il «rimedio preventivo» della consultazione tra Stati al fine di stabilire la «competenza più appropriata per l'esercizio dell'azione penale».

Nondimeno, nella misura in cui i progetti considerati agevoleranno lo svolgimento di attività ormai implicate dalla maggioranza dei procedimenti penali, e purché si realizzi un coordinamento tra le normative riferibili ai diversi ambiti dell'Unione europea, della Convenzione di Budapest, degli accordi con i Paesi terzi, si tratta di innovazioni che possono essere guardate con favore.

Sarà altresì la futura evoluzione delle proposte elaborate dalla Commissione, e l'eventuale applicazione pratica degli istituti a consentire di valutare se, effettivamente, il nuovo modello del contatto diretto con il privato – che comunque non pregiudica gli altri strumenti di cooperazione esistenti, quali l'OEI – sia tale da non tradire le aspettative.

Bibliografia:

Aa. Vv. (2011), *Computer forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici* (Forlì, Expert).

⁶⁵ DANIELE Marcello (2011), *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, 2, 287.

⁶⁶ *Ibidem*.

ALLEGREZZA Silvia (2018), “Prova scientifica e dimensione europea”, in CANZIO Giovanni, LUPARIA Luca (eds.), *Prova scientifica e processo penale*, (Padova, CEDAM), 117-157.

ALLEGREZZA Silvia, MOSNA Anna, NICOLICCHIA Fabio (2016), “L’acquisizione della prova all’estero e i profili transnazionali”, in CANZIO Giovanni, CERQUA Luigi Domenico, LUPARIA Luca (eds.), *Diritto penale delle società*, (Padova, CEDAM), pp. 157-192.

BELFIORE Rosanna (2015), “Riflessioni a margine della Direttiva sull’ordine europeo di indagine penale”, *Cassazione penale*, 2015, 9, 3288-3295.

CAMALDO Lucio (2014), “La direttiva sull’ordine europeo di indagine penale (OEI): un congegno di acquisizione della prova dotato di molteplici potenzialità, ma di non facile attuazione”, *Diritto penale contemporaneo*.

CERQUA Federico (2016), “Le indagini ad alta tecnologia per il contrasto della criminalità informatica”, in CANZIO Giovanni, CERQUA Luigi Domenico, LUPARIA Luca, *Diritto penale delle società*, (Padova, CEDAM), pp. 93-106.

COLAIACOVO Guido (2017), “Nuove prospettive in tema di coordinamento delle indagini e cooperazione giudiziaria alla luce della disciplina delle squadre investigative comuni”, *Rivista trimestrale Diritto penale contemporaneo*, 1, pp. 169-174.

Daniele Marcello (2017), “L’ordine europeo di indagine penale entra a regime. Prime riflessioni sul d. lgs. n. 108 del 2017”, *Diritto penale contemporaneo*, 7-8, pp. 208-215.

Daniele Marcello (2011), “La prova digitale nel processo penale”, *Rivista di diritto processuale*, 2, pp. 283-298.

Di Paolo Gabriella (2013), “Prova informatica (diritto processuale penale)”, in *Enciclopedia del diritto, Annali, VI*, (Milano, Giuffrè), pp. 736-762.

GIALUZ Mitja, DELLA TORRE Jacopo (2018), “Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali”, *Diritto penale contemporaneo*, 5, pp. 277-294.

KOSTORIS Roberto E. (2018), “Ordine di investigazione europeo e tutela dei diritti fondamentali”, *Cassazione penale*, 5, pp. 1437-1449.

MANGIARACINA Annalisa (2018), “L’acquisizione “europea” della prova cambia volto: l’Italia attua la Direttiva relativa all’ordine europeo di indagine penale. Commento a d.lg. 21 giugno 2017, n. 108”, *Diritto penale e processo*, 2, p. 159.

MARCHETTI Maria Riccarda (2018), “Ricerca e acquisizione probatoria all’estero: l’ordine europeo di indagine”, *Archivio penale*, 1S, p. 827.

NOCERA Andrea (2018), “Il sindacato giurisdizionale interno in tema di ordine europeo di intercettazione”, *Diritto penale contemporaneo*, pp. 149-168.

PEZZUTO Raffaella (2019), “Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell’Unione”, *Diritto penale contemporaneo*, 1, pp. 57-88.

PITTIRUTI Marco (2017), *Digital evidence e procedimento penale* (Torino, Giappichelli).

RUGGERI Stefano (2018), “Indagini e azione penale nei procedimenti di competenza della Procura europea”, *Processo penale e giustizia*, 3, pp. 602-616.

6.

SIGNORATO Silvia (2016), “Tipologie e caratteristiche delle *cyber investigations* in un mondo globalizzato”, *Rivista Trimestrale Diritto penale contemporaneo*, 3, pp.190-200.

SIRACUSANO Francesco (2017), “La prova informatica transnazionale: un difficile “connubio” fra innovazione e tradizione”, *Processo penale e giustizia*, 1, p. 18.

TINOCO PASTRANA Angel, “L’ordine europeo di indagine penale. Commento a Dir. UE 2014/41”, *Processo penale e giustizia*, 2017, 2, pp. 342-359.

TROGU MAURO (2018), “Ordine europeo di indagine penale”, in MARANDOLA Antonella (editor), *Cooperazione giudiziaria europea in materia penale* (Milano, Giuffrè), pp. 1004-1101.