L'acquisizione delle prove digitali dai *service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale

Digital Evidence gathering from service providers: a worrying paradigm shift in international cooperation

Obtenção de provas digitais por servidores: uma preocupante mudança de paradigma na cooperação internacional

Marcello Daniele[1]

Università degli Studi di Padova - Italia

marcello.daniele@unipd.it

http://orcid.org/0000-0002-8791-255X

Abstract: È sempre più frequente che le prove digitali rilevanti ai fini di un procedimento penale non siano localizzate nello Stato di commissione del reato, ma si trovino disperse nel *cloud*, risultando accessibili solo grazie all'intervento dei *service provider* che le detengono. In casi del genere i tradizionali strumenti di cooperazione giudiziaria entrano in crisi, poiché può diventare molto difficile individuare uno Stato di esecuzione a cui rivolgere le richieste istruttorie. Di qui l'idea, recepita da una proposta di regolamento dell'Unione Europea, di creare un canale di cooperazione diretta fra le autorità giudiziarie interessate all'acquisizione delle prove e i *provider*, a cui spetterebbe verificare che le richieste istruttorie rispettino la Carta di Nizza. Ne deriverebbe, però, la privatizzazione di un'attività tradizionalmente riservata ad organi pubblici: un preoccupante cambio di paradigma che rischia di porre in serio pericolo i diritti fondamentali.

Parole chiave: Prova digitale; cooperazione giudiziaria; diritti fondamentali.

[1] Professore ordinario di Diritto processuale penale.

Abstract: *It is becoming increasingly common that digital evidence relevant to criminal proceedings is not located in the State in which the crime was committed, but it is spread in the cloud computing, and it can be accessed only thanks to the intervention of the service providers that hold it. In such cases traditional instruments of judicial cooperation enter into crisis, since it can become very difficult to identify an executing State to which the evidence requests can be addressed. Hence the idea, implemented by a proposal for a European Union regulation, to create a channel of direct cooperation between the judicial authorities interested in acquiring the evidence and the providers, who would be responsible for verifying that the evidence requests respect the Charter of Nice. The result, however, is the privatization of an activity traditionally reserved to public bodies: a worrying paradigm shift that could put fundamental rights in serious danger.*

Keywords: *Digital Evidence; Judicial cooperation; fundamental rights.*

Resumo: *É cada vez mais frequente que as provas digitais relevantes para um processo penal não sejam localizadas no Estado em que ocorreu o cometimento de um crime, e que se encontrem dispersas no cloud, tornando-se dessa forma acessíveis somente por meio da intervenção do service provider que realiza o armazenamento. Nesses caos, os tradicionais instrumentos de cooperação judiciária entram em crise, porque pode tonar-se muito difícil especificar um Estado de execução ao qual direcionar pedidos de cooperação. Nesse quadro delineado, nasce a ideia, acolhida em uma proposta de regulamentação da União Europeia, de criar um canal de cooperação direta entre as autoridades judiciarias interessadas na colheita da prova e o provider, ao qual caberia verificar se os pedidos instrutórios respeitam a Carta de Nice. No entanto, trata-se de tendência de privatização de uma atividade tradicionalmente reservada aos órgãos públicos: uma preocupante mudança de paradigma capaz de fragilizar os direitos fundamentais.*

Palavras-chave: *Prova digital; cooperação judiciária; direitos fundamentais.*

Sommario: 1. Le prove digitali disperse nel *cloud*. 2. La cooperazione fra organi statali: una soluzione insoddisfacente. 3. Il nuovo paradigma della cooperazione diretta con i *service provider*. 4. La proposta di regolamento UE sull'ordine europeo di produzione e di conservazione delle prove digitali. 4.1. I limiti della proposta: a) le garanzie a geometria variabile. 4.2. b) La privatizzazione della tutela dei diritti fondamentali. 5. L'esigenza di un approccio federalistico. Bibliografia

1. Le prove digitali disperse nel *cloud*.

Non è raro che le prove digitali rilevanti ai fini di un procedimento penale si trovino in uno Stato diverso da quello di commissione del reato[2], sfuggendo così alla sovranità esclusiva di quest'ultimo. È una situazione a cui gli strumenti della cooperazione internazionale non riescono a rimediare, nella misura in cui – come sempre più spesso accade – si tratti di prove che circolano nello spazio virtuale del *cloud*[3], detenute da *service provider*: aziende private che offrono i più vari prodotti *online* (*email*, *social network*, *hosting*) a livello globalizzato, e la cui collaborazione si rivela, così, imprescindibile ai fini delle indagini. In alternativa, gli organi investigativi dovrebbero acquisire le prove con mezzi propri (ad esempio, tramite l'inoculazione di un *trojan* in un dispositivo in cui si presume che esse siano reperibili); con il rischio, però, di danneggiarle o contraffarle, pregiudicandone la spendibilità in giudizio[4].

Di qui l'esigenza di rimeditare il postulato – finora dato per scontato – secondo cui la cooperazione dovrebbe avvenire fra organi statali. Diventa indispensabile pensare a meccanismi in grado di includere anche i *provider*; ed è un compito non facile, se si considera che, come vedremo, richiede di coinvolgere in attività a rilevanza pubblica soggetti privati che, coadiuvando le autorità inquirenti, potrebbero rischiare di pregiudicare i propri interessi.

2. La cooperazione fra organi statali: una soluzione insoddisfacente.

Come è noto, gli attuali strumenti di cooperazione – la rogatoria e, nell'ambito dell'Unione Europea, la sua versione più evoluta, rappresentata

---

[2] Su questa loro caratteristica, v. M. Daniele, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2011, p. 285 s., e S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, p. 152 s.

[3] Cfr., al riguardo, S. Aterno, *Cloud forensics: aspetti giuridici e tecnici*, in Aa.Vv., *Cybercrime*, dir. da A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Utet, 2019, p. 1689 s.

[4] V. L. Bartoli, *Digital evidence for the criminal trial: limitless cloud and state boundaries, in Big data and Public Law: new challenges beyond data protection*, in *rivista.eurojus.it*, num. spec., 2019, p. 102.

dall'ordine europeo di indagine penale (OEI) [5] – sono fondati sulla collaborazione fra i competenti organi investigativi degli Stati coinvolti nelle operazioni istruttorie: lo Stato di emissione della richiesta, in cui vige la *lex fori*, e lo Stato di esecuzione, ossia quello in cui la prova è reperibile, in cui vale la *lex loci*. Così operando, però, non offrono una risposta soddisfacente al problema dell'acquisizione delle prove digitali nel *cloud*.

Anzitutto a causa della loro lentezza. Le norme che li regolano sono state concepite per le prove fisiche, e non sempre prevedono tempistiche di trasmissione adatte alla velocità con cui le prove digitali si muovono nella rete e possono trasmigrare da uno Stato ad un altro. La Convenzione di Budapest ne è consapevole, e richiede che le richieste istruttorie siano soddisfatte "al più presto possibile quando" "vi è motivo di ritenere che i dati relativi siano particolarmente a rischio di perdita o modificazioni" (art. 31 § 3), obbligando al contempo gli Stati a predisporre un "punto di contatto" fra le autorità "disponibile 24 ore su 24 e 7 giorni su 7" (art. 35). È possibile, poi, che le autorità interessate riducano i tempi attraverso appositi accordi informali. Rimane alto, nondimeno, il pericolo che la trasmissione delle prove non avvenga in tempo utile per una proficua fruizione delle prove da parte dello Stato di emissione.

Un altro limite è dovuto al fatto che, per funzionare al meglio, la rogatoria e l'OEI presuppongono la possibilità di individuare un unico Stato di esecuzione e, di conseguenza, una sola *lex loci*. È ricorrente, negli atti normativi che li disciplinano, la clausola secondo cui l'autorità di esecuzione deve attenersi alle "formalità" e alle "procedure" espressamente indicate dall'autorità di emissione sulla base della *lex fori*, salvo che queste ultime confliggano con i "principi fondamentali" della *lex loci*, o portino

[5] Le rogatorie sono disciplinate, in particolare, dalla Convenzione del Consiglio d'Europa di assistenza giudiziaria in materia penale del 1959, recepita dall'Italia con la l. 23 febbraio 1961, n. 215, nonché, nel contesto dell'Unione Europea, dalla Convenzione di assistenza giudiziaria in materia penale del 2000, recepita con il d.lgs. 5 aprile 2017, n. 52. Per quanto riguarda l'uso della rogatoria per la raccolta transnazionale delle prove digitali, poi, va menzionata la Convenzione del Consiglio d'Europa sulla criminalità informatica del 2001 (c.d. Convenzione di Budapest) L'OEI, dal canto suo, è disciplinato dalla direttiva 2014/41, recepita con il d.lgs. 21 giugno 2017, n. 108. Tutte queste prescrizioni sono integrate a livello nazionale, laddove non dispongano diversamente, dalle norme previste dagli artt. 723 s. c.p.p.

ad un'eccessiva compressione dei diritti fondamentali delle persone coinvolte[6]. Tale condizione – non esente da margini di ambiguità – se non altro mira ad evitare che le modalità di raccolta delle prove si appiattiscano su una *lex fori* non sufficientemente attenta alle garanzie, dando spazio ai superiori *standard* di tutela eventualmente previsti dalla *lex loci*, in una logica di contemperamento della sovranità dello Stato richiedente con quella dello Stato di esecuzione.

Ebbene, la dispersione delle prove digitali spesso porta alla moltiplicazione delle *lex loci*. Come identificare, in tali ipotesi, lo Stato di esecuzione? Dovrebbe essere lo Stato in cui opera o ha la sede legale il *service provider* che ha accesso alle prove? Oppure dovrebbe essere lo Stato in cui si trova il *server* dove le prove sono reperibili, magari diverso dallo Stato del *provider* [7]? E in quest'ultimo caso, come effettuare la scelta qualora, come spesso accade per ragioni economiche od organizzative, le prove vengano fatte costantemente circolare fra *server* situati in Stati diversi (c.d. *load balancing*) [8]?

A queste condizioni, è evidente come i vigenti strumenti di cooperazione giudiziaria diventino obsoleti. A fronte di una molteplicità di Stati a cui sarebbe possibile rivolgere la richiesta istruttoria, nessuno Stato, da solo, potrebbe fondatamente rivendicare il ruolo di Stato di esecuzione. Di qui il pericolo che quest'ultimo venga individuato in modo arbitrario o, comunque, sulla base di criteri incapaci di fornire una tutela adeguata delle garanzie: uno per tutti, il *forum shopping*, che consentirebbe all'autorità dello Stato di emissione di prescegliere lo Stato dotato del sistema di maggiori capacità repressive, e quindi più propenso a trasmettere le prove.

---

[6] Si vedano, per le rogatorie, gli artt. 4 della Convenzione del 2000 e 8 d.lgs. n. 52 del 2017, nonché, per l'OEI, gli artt. 9 § 2 direttiva 2014/41 e 4 comma 2 e 5 comma 3 d.lgs. n. 108 del 2017. Cfr. anche l'art. 27 § 3 della Convenzione di Budapest.

[7] Come accaduto, ad esempio, nel noto caso *Microsoft Ireland*, in cui un'autorità giudiziaria statunitense aveva chiesto alla Microsoft, azienda statunitense, alcuni dati reperibili in un *server* situato in Irlanda.

[8] Su queste variabili v. J. Daskal, *Borders and bits*, in *71 Vanderbilt Law review*, 2018, p. 190; S. Signorato, *Le indagini digitali*, cit., p. 199 s.; F. Siracusano, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, in *Proc. pen. giust.*, f. 1, 2017, p. 180 ss.

3. Il nuovo paradigma della cooperazione diretta con i *service provider*

Visti i limiti della cooperazione fra organi statali, non stupisce che, nella prassi, abbia preso piede un metodo alternativo: la richiesta diretta da parte dell'autorità giudiziaria interessata alle prove ai *service provider* che le detengono, senza coinvolgere nessun altro Stato.

È un metodo che, allo stato, non trova una specifica regolamentazione. Non appare consentito rinvenirne un embrione operativo nell'art. 234 *bis* c.p.p., che ha trasposto nel nostro sistema l'art. 32 della Convenzione di Budapest. È vero che tale disposizione prescrive, laconicamente, che è "sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare". Quest'ultimo, tuttavia, non potrebbe essere identificato con chi, come un *service provider*, detenga dati altrui[9]; diversamente, si introdurrebbe la possibilità di ottenere i dati aggirando le vigenti norme sulla cooperazione. Né va trascurato che quello del consenso è, per intuibili ragioni, comunque un requisito difficile da soddisfare[10].

Non essendo regolata, la cooperazione diretta con i *provider*, attualmente, si fonda sulla *voluntary disclosure*: ciascuna azienda decide di volta in volta, sulla base dei propri interessi, se ed entro quali limiti collaborare. Il che spiega perché l'Unione Europea, ora, vorrebbe disciplinarla; un intento che si è concretizzato in una proposta tuttora in fase di gestazione[11], volta ad introdurre strumenti istruttori che, veicolati da un regolamento anziché da una direttiva, non avrebbero bisogno di

---

[9] Cfr. D. Negri, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in *Arch. pen.*, f. 3, 2015, p. 53.

[10] V. J. Spoenle, *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?*, in *coe.it*., 31 agosto 2010, p. 7.

[11] "*Proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*" del 17 aprile 2018 (COM(2018) 225 final). In merito ad alcune possibili modifiche della proposta, v. R. Pezzuto, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, in *penalecontemporaneo.it*, f. 1, 2019, p. 67 s.

un'implementazione nazionale, ma sarebbero direttamente operanti nei singoli Stati, evitando di trovare declinazioni diverse nei vari sistemi[12].

Sullo sfondo di un intervento del genere vi è un cambio di paradigma della filosofia della cooperazione giudiziaria di non poco conto. I nuovi congegni non sostituirebbero, ma si affiancherebbero alla rogatoria e all'OEI, ampliando così le possibilità per le autorità giudiziarie dell'Unione di venire in possesso delle prove digitali non disponibili nei propri paesi[13]. Non è difficile prevedere, tuttavia, che, grazie alla loro maggiore efficacia applicativa, essi assumerebbero un'importanza preminente. È fondamentale, dunque, prendere coscienza dei limiti che li contraddistinguono.

4. La proposta di regolamento UE sull'ordine europeo di produzione e di conservazione delle prove digitali

In sintesi, la nuova modalità di cooperazione delineata dalla proposta di regolamento si basa sui seguenti capisaldi.

i) Vengono disciplinate due tipologie di richieste: l'ordine di produzione, mirato alla trasmissione dei dati; l'ordine di conservazione, finalizzato invece alla custodia dei dati in vista di una successiva richiesta di produzione, impedendone temporaneamente la cancellazione o la modifica.

ii) Gli ordini possono essere rivolti dalle competenti autorità nazionali direttamente ai rappresentanti legali dei *provider* che offrono i loro servizi nell'Unione Europea. Questi ultimi possono ricomprendere i

---

[12] Cfr. 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 *penalecontemporaneo.it*, f. 5, 2018, p. 292.

[13] Gli ordini di produzione e di conservazione non potrebbero, peraltro, essere utilizzati per effettuare intercettazioni, le quali continuerebbero a richiedere l'emissione di una rogatoria o di un OEI. Una restrizione comprensibile, in quanto dovuta all'esigenza di evitare di trasformarli in strumenti di prevenzione o, peggio, di sorveglianza occulta, nonché di addossare un (economicamente gravoso) dovere di monitoraggio continuo a carico dei *provider*: v. O. Pollicino-M. Bassini, *La proposta di Regolamento e-Evidence: osservazioni a caldo e possibili sviluppi*, in *medialaws.ue*, 26 ottobre 2018, p. 15.

fornitori sia di servizi di comunicazione elettronica (*email*), sia di servizi della c.d. società dell'informazione (come i *social network* o i prestatori di servizi di *hosting*), o di nomi di dominio *internet* e di numerazione IP (art. 2 della proposta).

iii) Gli ordini possono avere ad oggetto due tipologie di dati: quelli relativi agli "abbonati" e agli "accessi" da un lato, e quelli relativi alle "operazioni" e al "contenuto" dall'altro.

iv) Sono previste diverse condizioni tanto per l'emissione quanto per l'esecuzione degli ordini (artt. 4-10).

v) Soddisfatte tali condizioni, gli ordini di produzione vanno eseguiti rispettando tempistiche serrate: dieci giorni o, in caso di urgenza, addirittura sei ore dalla loro ricezione (art. 9); la conservazione dei dati, dal canto suo, deve iniziare immediatamente, per durare di regola sessanta giorni (art. 10).

vi) Quando, pur ricorrendone le condizioni, gli ordini non vengano eseguiti entro i termini previsti, i *provider* possono essere sottoposti a sanzioni pecuniarie da parte degli Stati in cui essi hanno la loro sede legale (artt. 13 e 14).

vii) Ai titolari dei dati, a prescindere dal fatto che siano persone sottoposte ad un procedimento penale o terzi, deve essere assicurato un mezzo di impugnazione esperibile nello Stato di emissione al fine di contestare le legittimità degli ordini di produzione (art. 17).

Si vorrebbe, in tal modo, creare un canale di cooperazione rapida ed efficace con chi detiene i dati, eliminando le lungaggini che, inevitabilmente, deriverebbero dall'esigenza di coinvolgere un altro Stato nelle operazioni istruttorie. Peraltro, come emerge dall'art. 1 § 2[14], i compilatori della proposta sono consapevoli del fatto che si tratta di attività suscettibili di interferire con i diritti fondamentali degli individui. Basti menzionare, fra questi, il diritto al rispetto alla vita privata (artt. 8 CEDU e 7 Carta di Nizza) e la libertà di espressione dei titolari dei dati

[14] Ai sensi del quale "il presente regolamento non ha l'effetto di modificare l'obbligo di rispettare i diritti fondamentali e i principi giuridici sanciti dall'articolo 6 TUE, compresi i diritti di difesa delle persone sottoposte a procedimento penale, e lascia impregiudicati gli obblighi spettanti a tale riguardo alle autorità di contrasto o giudiziarie".

(artt. 11 Carta di Nizza), nonché la libertà di iniziativa economica (art. 16 Carta di Nizza) dei *provider*.

Ne discende l'esigenza di rispettare, in particolare, il requisito della "necessità in una società democratica", richiesto dall'art. 8 § 2 CEDU ai fini del rispetto del diritto alla riservatezza. Il che, stando alla consolidata interpretazione della Corte europea dei diritti dell'uomo[15] e della Corte di giustizia dell'Unione Europea[16], si traduce nella "proporzionalità" delle misure da adottare: una condizione che presuppone l'impiego di garanzie processuali "adeguate e sufficienti contro l'abuso e l'arbitrarietà"[17], tali da assicurare che la compressione del diritto risulti strettamente indispensabile e, allo stesso tempo, non ne intacchi il nucleo essenziale.

Nei sistemi nazionali, queste garanzie si identificano, a seconda dei casi, con l'autorizzazione (preventiva o, perlomeno, successiva) delle operazioni istruttore da parte di un organo giurisdizionale, l'attinenza del procedimento ad un reato di una certa gravità e la sussistenza di indizi di colpevolezza. Come ora vedremo è, tuttavia, dubbio che la proposta di regolamento riesca pienamente ad assicurarle.

4.1. I limiti della proposta: a) le garanzie a geometria variabile.

La peculiarità della proposta consiste nell'adozione di un approccio a "geometria variabile", mirato a dosare le garanzie processuali in base alla tipologia di ordine da emettere e alle caratteristiche dei dati di interesse dell'autorità di emissione.

In generale tutti gli ordini, qualunque sia il loro contenuto, devono essere "necessari" e "proporzionati" (artt. 5 § 2 e 6 § 2). Questi due requisiti, di per sé piuttosto generici[18], assumono contorni più precisi se li si identifica con le condizioni di emissione dei corrispondenti atti istruttori che, in base alla *lex fori*, opererebbero a livello nazionale. Nel nostro

---

[15] V., fra le molte, Corte eur. dir. uomo, GC., 4 dicembre 2015, *Roman Zakharov c. Russia*, § 227 s.; Id., GC, 4 maggio 2000, *Rotaru c. Romania*, § 47 s.

[16] Cfr. Corte giustizia U.E., 8 aprile 2014, *Digital Rights Ireland*, C-293/12 e C-594/12, § 38 s.

[17] Corte eur. dir. uomo, 27 settembre 2018, *Brazzi c. Italia*, § 41.

[18] V. M. Gialuz-J. Della Torre, *Lotta alla criminalità*, cit., p. 293.

sistema, viene in gioco il presupposto di emissione delle perquisizioni informatiche (art. 247 comma 1 *bis* c.p.p.), ossia il "fondato motivo" di ritenere che dati "pertinenti al reato" oggetto del procedimento siano rinvenibili in un determinato spazio informatico o siano detenuti da un certo *service provider*.

Gli ordini di produzione, inoltre, possono essere emessi solo se "una misura dello stesso tipo è disponibile per lo stesso reato in una situazione nazionale comparabile nello stato di emissione" (artt. 5 § 2). Il che significa che la legge deve contemplare la possibilità per gli organi inquirenti di svolgere indagini informatiche al fine di acquisire prove digitali detenute dai *provider*: una facoltà, in Italia, disciplinata dall'art. 254 *bis* c.p.p.

Ciò detto, se gli ordini meno problematici dal punto di vista del rispetto della *privacy* – ossia gli ordini di conservazione e gli ordini di produzione dei soli dati relativi agli abbonati o agli accessi – possono essere disposti in rapporto a qualsiasi reato (artt. 6 § 2 e 5 § 3), per gli ordini di produzione dei dati relativi alle operazioni e al contenuto – in linea di massima, ben più invasivi – è necessario che il procedimento abbia ad oggetto un reato punibile nello Stato di emissione con una pena detentiva di almeno tre anni, oppure uno dei gravi reati appositamente elencati dalla proposta (art. 5 § 4).

Il limite edittale dei tre anni, piuttosto basso, consente di ricomprendere la maggioranza delle fattispecie penali[19], nella sostanza annullando sotto questo profilo ogni differenza fra gli ordini più invasivi e quelli meno invasivi. Ma non è, tutto sommato, un difetto grave, se si pensa al fatto che, a livello interno, le indagini informatiche possono essere svolte in rapporto a qualsiasi tipo di reato.

Appare comprensibile, inoltre, la scelta di rinunciare al tradizionale requisito della doppia incriminazione. Ad esso deroga già la disciplina sull'ordine europeo di indagine penale, la quale consente la raccolta delle prove all'estero in rapporto a tutti i reati appositamente elencati in una lista (artt. 11 § 1 lett. *g* della direttiva 2014/41 e 11 d.lgs. n. 108/2017): illeciti che, punibili nello Stato di emissione con una pena di almeno tre anni di detenzione, sono considerati di gravità tale da giustificare per definizione

[19] Cfr. L. Bartoli, *Digital evidence*, cit., p. 105.

le operazioni istruttorie. Soprattutto, il più sopra menzionato fenomeno di possibile moltiplicazione della *lex loci* determinato dalla dispersione delle prove digitali rende la doppia incriminazione un criterio, spesso, inapplicabile, come tale da considerare superato.

Non appare censurabile neppure la possibilità per l'autorità di emissione di chiedere al *provider* di astenersi dall'"informare la persona i cui dati sono ricercati, per non ostacolare il pertinente procedimento penale" (art. 11 § 1 della proposta), ritardando l'informazione al momento in cui non vi sia più il rischio di compromettere le indagini[20]. Qualcosa del simile avviene già a livello nazionale, laddove vi è tutta una serie di atti "a sorpresa" che possono essere disposti dall'organo di accusa senza previamente informare il difensore (si pensi alle perquisizioni): una cautela indispensabile per evitare il rischio di pregiudicare l'efficace compimento dell'atto.

La proposta risulta, per converso, eccepibile nella misura in cui non assicura una piena attuazione del controllo giurisdizionale. Non va infatti dimenticato che, stando alla giurisprudenza della Corte europea dei diritti dell'uomo, la sottoposizione delle operazioni istruttorie invasive della *privacy* ad un vaglio – almeno successivo – di un organo indipendente rappresenta uno degli elementi del nocciolo duro del diritto[21]. Eppure la proposta introduce, a questo riguardo, tutta una serie di distinzioni. Un vaglio giurisdizionale preventivo è assicurato per i soli ordini di produzione dei dati relativi alle operazioni e al contenuto (art. 4 § 2). Per gli ordini di produzione dei dati relativi agli abbonati e agli accessi – che in prima battuta possono essere disposti anche solo da un pubblico ministero (art. 4 § 1) – ci si accontenta, invece, di un ricorso *ex post* "davanti ad un organo giurisdizionale dello Stato di emissione" in conformità alla *lex fori* (art.

---

[20] Per una critica v. invece, O. Pollicino-M. Bassini, *La proposta*, cit., p. 18.

[21] Lo ha ribadito, fra le più recenti, Corte eur. dir. uomo, 27 settembre 2018, *Brazzi c. Italia*, § 1 s. relativa ad una perquisizione di un'abitazione e dei *personal computer* ivi rinvenuti disposta da un pubblico ministero in un procedimento per evasione fiscale. La mancanza di un'autorizzazione preventiva di un giudice – non richiesta, a livello interno, dall'art. 247 c.p.p. – è stata giudicata dalla Corte europea incompatibile con l'art. 8 CEDU per la ragione che alla perquisizione non era seguito nessun sequestro, e dunque l'interessato non aveva potuto esperire il riesame ai sensi dell'art. 257 c.p.p. (in modo da attivare un vaglio giurisdizionale perlomeno posticipato).

17 § 3) [22]: una disparità di trattamento che, a ben guardare, non risulta giustificata, se si considera che gli ordini di produzione hanno ad oggetto categorie di dati per alcuni versi sovrapponibili[23]. Possono essere emessi da un pubblico ministero (art. 4 § 3) senza un controllo giurisdizionale nemmeno successivo, infine, gli ordini di conservazione, ed è una scelta difficilmente comprensibile. Per quanto questi ultimi non consentano la "divulgazione dei dati" [24], nondimeno pregiudicano la facoltà del titolare di modificarli ed usarli liberamente[25]. Il fatto che non siano in nessun modo impugnabili, oltretutto, determina un'evidente tensione con il diritto ad un ricorso effettivo previsto dall'art. 47 della Carta di Nizza[26].

4.2. b) La privatizzazione della tutela dei diritti fondamentali.

L'aspetto più preoccupante della proposta consiste nell'affidare ai *provider* – aziende private e non organi pubblici – il controllo sull'eseguibilità degli ordini.

Gli argomenti a sostegno di tale soluzione sono, essenzialmente, di tipo utilitaristico. Si osserva, in particolare, che i *provider* a cui gli ordini sono rivolti svolgono, sia pure virtualmente, un'attività economicamente redditizia nello Stato di emissione, nel quale hanno collocato la loro sede operativa magari per ragioni fiscali. Sarebbe la giurisdizione di quest'ultimo, pertanto, a venire principalmente in gioco ai fini dello svolgimento delle attività istruttorie. Né va dimenticato che la raccolta

---

[22] Il quale sia tale da includere "la possibilità di contestare la legittimità della misura, comprese la sua necessità e la sua proporzionalità".

[23] Si pensi, in particolare, ai dati sulle operazioni (ad esempio, come chiarisce l'art. 2 § 7 della proposta, la "fonte e il destinatario di un messaggio", o "altro tipo di interazione"), che potrebbero facilmente essere scambiati per dati sugli accessi (ossia quelli riguardanti "l'inizio o la fine di una sessione di accesso al servizio"), fruendo così del livello di garanzia inferiore; oppure ai dati relativi alla cronologia di ciascun utente o alle ricerche effettuate, in rapporto a cui sorgerebbero non pochi dubbi di collocazione e, quindi, sulle garanzie da applicare: V. O. Pollicino-M. Bassini, *La proposta*, cit., p. 14.

[24] Così la spiegazione dell'art. 17 della proposta.

[25] Cfr. M. Gialuz-J. Della Torre, *Lotta alla criminalità*, cit., p. 292.

[26] V. R.M. Geraci, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di regolamento di* e-evidence, in *Cass. pen*., 2019, p. 1360.

delle prove digitali tramite gli ordini di conservazione e di produzione non comporta nessun ingresso fisico da parte degli organi inquirenti dello Stato di emissione in un altro Stato, la cui sovranità non potrebbe, dunque, considerarsi realmente lesa[27].

Non è facile sostenere, tuttavia, che l'esclusione dai giochi degli organi pubblici dello Stato di esecuzione sia del tutto indolore. I criteri di controllo da impiegare ai fini dell'eseguibilità degli ordini di produzione e di conservazione sono, nella sostanza, non molto diversi da quelli utilizzabili dalle autorità giudiziarie chiamate ad eseguire le rogatorie e gli OEI. E se si considera che fra essi rileva la "manifesta violazione" della Carta di Nizza o la "manifesta arbitrarietà" (art. 14 commi 4 e 5 della proposta), è evidente come il vaglio del rispetto dei diritti fondamentali finisca per essere privatizzato.

Non si tratta, peraltro, di una peculiarità della proposta. Una prescrizione non dissimile si riscontra nel *CLOUD Act* del 2018, l'omologo statunitense del regolamento eurounitario, il quale prescrive che i *provider* potrebbero rifiutarsi di trasmettere i dati in presenza di un "rischio effettivo" di violazione del diritto di uno Stato straniero (§ 103[28]). Non dissimile il discorso per quanto concerne, più in generale, la tutela della *privacy* digitale a livello europeo; basti pensare al diritto alla deindicizzazione dei contenuti rinvenibili nei siti, anche esso sottoposto allo scrutinio delle aziende private che gestiscono i motori di ricerca[29].

Ci troviamo, dunque di fronte ad un *trend* che si sta imponendo a livello globale, e che proprio per questo deve essere considerato con la massima cautela. Vi è chi lo guarda con favore, notando come l'eliminazione del controllo da parte dei competenti organi dello Stato di esecuzione semplifichi non poco la procedura, con l'effetto di aumentare l'efficienza delle investigazioni. Inoltre i *service provider* – secondo questa impostazione – si troverebbero nella migliore posizione per effettuare il controllo, vuoi perché dotati delle specifiche competenze tecniche necessarie al riguardo, vuoi perché in possesso delle informazioni

---

[27] Cfr., al riguardo, P. de Hert-C. Parlar-J. Thumfart, *Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to Microsoft Ireland*, in *New Journal of European Criminal Law*, vol. 9 (3), 2018, p. 338 s.

[28] La quale ha modificato la § 2713, tit. 18, cap. 121 dello *United States Code*.

[29] Cfr. O. Pollicino-M. Bassini, *La proposta*, cit., p. 10 s.

rilevanti. Si tratterebbe, del resto, di un vaglio fondato su indici giuridici "di agevole riconoscibilità anche per operatori privati", tali da non implicare necessariamente "l'esigenza di un apprezzamento di carattere tecnico" [30].

In caso di pericolo di violazione dei diritti – si conclude – comunque opererebbe un'ancora di salvataggio: la procedura di riesame prevista dall'art. 15 della proposta, attivabile quando il *provider* ritenga che l'ottemperanza di un ordine di produzione sia in contrasto con il diritto di un paese terzo che vieti la divulgazione dei dati "per la necessità di tutelare i diritti fondamentali delle persone interessate". In evenienze del genere, un organo giurisdizionale dello Stato di emissione dovrebbe riconsiderare la situazione e, se accertasse l'esistenza di una possibile violazione, dovrebbe interpellare il paese terzo, il quale potrebbe anche arrivare ad opporsi all'esecuzione dell'ordine. In questo modo, i *provider* diventerebbero "il perno centrale del sistema, fungendo da valvola in grado di regolare l'ingresso di un determinato ordine proveniente dall'autorità di emissione di uno Stato membro nell'ordinamento in cui i dati oggetto di ricerca sono materialmente conservati" [31].

Ci sono, tuttavia, forti dubbi che un tale complesso meccanismo possa sortire i suoi effetti, e ciò per una ragione connessa alla stessa essenza dei *provider*: i quali, a causa della loro natura privatistica e della conseguente – e legittima – esigenza di proteggere i loro interessi, non potrebbero mai agire come organi pubblici in posizione di imparzialità, di per sé del tutto indifferenti all'esito del vaglio[32]. Per quanto possano avere a cuore la tutela della *privacy* dei loro utenti, la loro condotta sarebbe condizionata dalla comprensibile necessità di mantenere buoni rapporti con gli Stati in cui esercitano la loro attività economica. Il

---

[30] O. Pollicino-M. Bassini, *La proposta*, cit., p. 17.

[31] O. Pollicino-M. Bassini, *La proposta*, cit., p. 11.

[32] Cfr. M. Böse, *An assessment of the Commission's proposals on electronic evidence*, in *europarl.europa.eu*, 21 settembre 2018, p. 41 s.; 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*, vol. 25 (3), 2018, p. 264 s. Si veda anche il *3rd working document* del Parlamento europeo sulla proposta di regolamento del 13 febbraio 2019, in *europarl.europa.eu*, p. 5 s., nonchè P. de Hert-C. Parlar-J. Thumfart, *Legal arguments*, cit., p. 351 s., secondo cui la proposta è più attenta alle esigenze repressive che alla tutela della sovranità degli Stati coinvolti e dei diritti degli individui.

rischio, poi, che, rifiutandosi di eseguire gli ordini di conservazione o produzione dei dati, siano esposti a sanzioni, inevitabilmente falserebbe le loro valutazioni. Non ci sarebbe da stupirsi, a queste condizioni, se svolgessero un vaglio superficiale, censurando solo le (probabilmente poche) istanze di acquisizione patentemente lesive dei diritti, in quanto prive di qualsiasi giustificazione (si pensi alle c.d. *fishing expeditions*, richieste "al buio" volte a sapere quali dati siano in mano ad un certa azienda). Un tendenziale lassismo a cui contribuirebbero i rapidi tempi di risposta imposti dalla proposta, nonché il fatto che, stando all'art. 8 commi 3 e 4 di quest'ultima, gli appositi certificati mediante cui gli ordini dovrebbero essere trasmessi ai *provider* non dovrebbero includere "i motivi della necessità e della proporzionalità della misura", ostacolando il controllo anche sotto questo profilo[33].

Così stando le cose, il rispetto dei diritti fondamentali sarebbe, alla resa dei conti, devoluto al solo Stato di emissione sulla base del proprio ordinamento, venendo meno qualsiasi forma di tutela delle legittime aspettative del titolare dei dati in merito all'applicazione della normativa di qualsiasi altro Stato coinvolto. Tale unica salvaguardia, però, potrebbe risultare inadeguata qualora la *lex fori* non fosse sufficientemente attenta alle esigenze garantistiche. Anche perché non va trascurato che l'art. 17 § 6 della proposta, riprendendo la medesima soluzione adottata dall'art. 14 § 7 della direttiva 2014/41 sull'ordine europeo di indagine penale, dispone che le violazioni del diritto di difesa e del diritto all'equo processo sono destinate a ripercuotersi solo sulla "valutazione" delle prove ottenute. Una prescrizione del genere non potrebbe che tradursi in una regola volta ad attribuire alle prove in questione un peso conoscitivo inferiore, magari tipo quella prevista, a livello interno, dall'art. 192 comma 3 c.p.p. in rapporto alle dichiarazioni dei coimputati[34]. Ma l'esperienza applicativa ha da tempo dimostrato come prescrizioni del genere siano poco efficaci, prestandosi a tutta una serie di elusioni consentite dall'elasticità della logica induttiva che governa l'accertamento dei fatti[35]. A fronte della

[33] Si veda il *3rd working document* del Parlamento europeo, p. 4.

[34] Le quali, viste dal nostro legislatore con sospetto, come noto devono essere assistite da specifici elementi di riscontro.

[35] Si rinvia a M. Daniele, *Regole di esclusione e regole di valutazione*, Giappichelli, 2009, p. 132 s.

lesione dei diritti fondamentali, la via più corretta sarebbe quella di decretare l'inutilizzabilità delle prove. Tale più radicale sanzione, però, è prevista come mera eventualità dal *considerando* 54 della proposta[36], non potendo dunque essere considerata una strada vincolata per i giudici nazionali chiamati ad applicare il regolamento.

5. L'esigenza di un approccio federalistico

Se la cooperazione fra organi pubblici risulta un passaggio ineludibile, ci si deve chiedere come rivitalizzarla, in modo da renderla compatibile con le caratteristiche delle prove digitali.

Nulla vieterebbe alla legge di individuare un unico Stato di esecuzione. Qui le soluzioni potrebbero essere molteplici. Lo si potrebbe identificare, ad esempio, con lo Stato in cui il *provider* ha la sede legale, oppure con lo Stato in cui si trova il *server* in cui sono ubicate le prove o, addirittura, con lo Stato indicato dallo stesso *provider*; in alternativa, ci si potrebbe riferire allo Stato di nazionalità del sospettato, o allo Stato di nazionalità della vittima[37]. A causa della dispersione delle prove digitali, tuttavia, qualunque scelta sarebbe arbitraria o, comunque, foriera di complicazioni, e quindi insoddisfacente.

Nello scenario "liquido" delle indagini informatiche, l'approccio meno problematico passa attraverso la creazione, in una logica federale, di un unico organo giurisdizionale europeo deputato a svolgere i controlli che la proposta vorrebbe affidare ai *provider*[38]. Un organo a cui le autorità giudiziarie nazionali dovrebbero rivolgere gli ordini di conservazione e di produzione, e a cui i *provider* che prestino i loro servizi nell'Unione dovrebbero trasmettere le informazioni rilevanti in loro possesso.

---

[36] Secondo cui la violazione dei diritti "può incidere sull'ammissibilità delle prove ottenute con detti mezzi o, a seconda del caso, sul peso di tali prove nell'ambito del procedimento".

[37] Per una rassegna, v. A.K. Woods, *Against Data Exceptionalism*, in *68 Stanford Law Review*, 2016, p. 764 s.

[38] In merito a questo tipo di soluzione, v. 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*, Centre for European Policy Studies, 2015, p. 14 s.

Dovrebbe spettargli, in particolare, valutare se le richieste istruttorie rispettano gli *standard* di tutela dei diritti richiesti dalla CEDU e dalla Carta di Nizza; non potrebbe esimersi, a questo proposito, dal considerare la gravità dei reati oggetto del procedimento, le modalità e le circostanze di emissione del provvedimento, la presenza di elementi di prova a carico del sospettato già presenti in quel momento, nonché il contenuto e la finalità del provvedimento[39].

Non sarebbe, naturalmente, una soluzione priva di difetti. Dovrebbe essere un organo in grado di operare con la massima efficienza, capace di soddisfare in tempi ragionevolmente rapidi richieste provenienti da ogni parte del globo. A questo fine potrebbe forse essere utile prevedere, nei casi di urgenza, una procedura velocizzata: gli ordini che non apparissero manifestamente arbitrari potrebbero essere immediatamente eseguiti, per poi venire sottoposti ad un più approfondito vaglio successivo all'esecuzione, decretando *ex post* l'inutilizzabilità nello Stato di emissione dei dati raccolti qualora quest'ultimo avesse esito negativo[40]. In ogni caso, per quanto possa apparire difficile da realizzare, sarebbe una soluzione di gran lunga preferibile alla logica privatistica postulata dalla proposta di regolamento, suscettibile di aprire scenari dalle implicazioni davvero inquietanti per la tutela dei diritti.

Bibliografia

ATERNO, Stefano. Cloud forensics: aspetti giuridici e tecnici. In CADOPPI Alberto, CANESTRARI Stefano, MANNA Adelmo, PAPA Michele (a cura di). *Cybercrime*. Torino: Utet, 2019, p. 1689 s.

BARTOLI, Laura. Digital evidence for the criminal trial: limitless cloud and state boundaries. *Big data and Public Law: new challenges beyond data protection*, *rivista.eurojus.it*, 2019, num. spec., p. 96 s.

[39] Cfr. Corte eur. dir. uomo, 6 ottobre 2016, *K.S. e M.S. c. Germania*, § 44. V. anche Id., GC, 4 dicembre 2015, *Roman Zakharov*, cit., § 260, la quale richiede, ai fini delle intercettazioni, la presenza di un "ragionevole sospetto" a carico della persona sotto procedimento.

[40] Secondo un meccanismo non dissimile da quello adottato dall'art. 31 § 3 della direttiva sull'OEI in merito alle intercettazioni all'estero effettuate senza l'assistenza tecnica dello Stato straniero interessato.

BÖSE, Martin. *An assessment of the Commission's proposals on electronic evidence*. *europarl.europa.eu*, 21 settembre 2018.

CARRERA, Sergio, GONZÁLEZ FUSTER, Gloria, GUILD, Elspeth, MITSILEGAS, Valsamis. *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights*, Brussels: Centre for European Policy Studies, 2015.

DANIELE, Marcello. La prova digitale nel processo penale. *Rivista di diritto processuale*. Padova, p. 283 s., 2011.

DANIELE, Marcello. *Regole di esclusione e regole di valutazione*, Torino: Giappichelli, 2009.

DASKAL, Jennifer. Borders and bits, *71 Vanderbilt Law Review*. p. 179 s., 2018.

DE HERT, Paul, PARLAR, Cihan, THUMFART, Johannes. Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to Microsoft Ireland. *New Journal of European Criminal Law*, v. 9 (3), p. 326 s., 2018.

GERACI, Rosa Maria. La circolazione transfrontaliera delle prove digitali in UE: la proposta di regolamento di e-evidence. *Cassazione penale*, p. 1340 s., 2019.

GIALUZ Mitja, DELLA TORRE Jacopo. Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali. *Penalecontemporaneo.it*, f. 5, p. 277 s., 2018.

MITSILEGAS, Valsamis. The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence, *Maastricht Journal of European and Comparative Law*, vol. 25 (3), p. 263 s., 2018.

NEGRI, Daniele. La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico). *Archivio penale*, f. 3, p. 44 s., 2015.

PEZZUTO, Raffaella. Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione. *Penalecontemporaneo.it*, f. 1, p. 57 s., 2019.

POLLICINO, Oreste, BASSINI, Marco. La proposta di Regolamento e-Evidence: osservazioni a caldo e possibili sviluppi. *Medialaws.ue*, 26 ottobre 2018.

SIGNORATO, Silvia. *Le indagini digitali*. Profili strutturali di una metamorfosi investigativa. Torino: Giappichelli, 2018.

SIRACUSANO, Fabrizio. La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione, *Processo penale e giustizia*, f. 1, p. 178 s. 2017.

SPOENLE, Jan. Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal? C*oe.it*, 31 agosto 2010.

WOODS, Andrew Keane. Against Data Exceptionalism. *68 Stanford Law Review*, p. 279 s., 2016.

Informações adicionais e declarações dos autores (*integridade científica*)

Declaração de conflito de interesses (conflict of interest declaration): o autor confirma que não há conflitos de interesse na realização das pesquisas expostas e na redação deste artigo.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste artigo estão listadas como autores.

Declaração de ineditismo e originalidade (declaration of originality): o autor assegura que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atesta que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 22/08/2019
- Controle preliminar e verificação de plagio: 1/09/2019
- Avaliação 1: 16/09/2019
- Avaliação 2: 27/09/2019
- Decisão editorial preliminar: 21/09/2019
- Retorno rodada de correções: 04/10/2019
- Decisão editorial final: 08/10/2019

Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editoras-associadas: 2 (CC e BC)
- Revisores: 2

COMO CITAR ESTE ARTIGO:

DANIELE, Marcello. L'acquisizione delle prove digitali dai *service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1277-1296, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.288