ISSN 2384-9169
Fascicolo n. 2 - 2020
rivista.eurojus.it

Regolamento europeo e-evidence
Deficitario dal punto di vista dello stato di diritto, superato dalla realtà e a lungo termine in contrasto con gli interessi europei

DI CHRISTOPH BURCHARD*

Sommario: 1. Introduzione – 2. Presa di posizione rispetto alla proposta – 2.1. Elaborazione deficitaria dal punto di vista dello stato di diritto – 2.2. Distante dalla realtà in quanto basato su una differenziazione giuridica superata – 2.3. Pregiudizio a legittimi interessi di sicurezza degli Stati membri dell'Unione Europea – 3. Possibili soluzioni – 3.1. Scelta della base giuridica – 3.2. Disciplina processual-penale – 3.3. Disciplina intergovernativa – 3.4. Nessuna rinuncia alla cooperazione internazionale in materia di sicurezza – 4. Riflessioni conclusive.

1. Introduzione.

Il 7 dicembre 2018 il Consiglio dell'Unione europea – Giustizia e affari interni – ha approvato, contro il parere della Repubblica federale tedesca[1], una posizione comune concernente la direzione da seguire rispetto alle ulteriori negoziazioni con il Parlamento europeo su un regolamento relativo agli ordini europei di produzione e di conservazione di

* Titolare della Cattedra di Diritto e procedura penale, diritto penale europeo e internazionale, diritto comparato e teoria del diritto presso l'Università Goethe di Francoforte sul Meno. Il testo riproduce il contributo dal titolo *Europäische E-Evidence Verordnung. Rechstaatlich defizitär, der Realität hinterher und langfristig konträr zu europäischen Interessen* apparso in *Zeitschrift für Rechtspolitik* (2019) e tradotto dal tedesco all'italiano dal dott. Andrea Galante, Dottore di ricerca in Discipline penalistiche presso l'Università di Firenze e l'Università Goethe di Francoforte sul Meno.

[1] La decisione, inoltre, non ha trovato il supporto da parte di Finlandia, Grecia, Lettonia, Paesi Bassi, Repubblica Ceca e Ungheria. Si v. https://www.reuters.com/article/us-eu-tech-eevidence/eu-governments-agree-totougher-stance-on-e-evidence-idUSKBN1O6271. Che un importante atto giuridico della cooperazione giudiziaria penale nello spazio di libertà, sicurezza e giustizia sia stato affrontato in modo controverso all'interno del Consiglio è una assoluta novità e dovrebbe far riflettere.

prove elettroniche in materia penale (*E-Evidence*)[2]. Questo progetto di regolamento è attualmente oggetto di un'intensa (e piuttosto critica) elaborazione in seno al Parlamento europeo[3], mentre in Germania sia il *Bundesrat* (Senato federale)[4] che il governo federale tedesco[5] hanno manifestato preoccupazione con riferimento ad esso, seppur in termini diplomaticamente *soft*. Inoltre, quest'ultimo ha ricevuto un'accoglienza prevalentemente negativa sia da parte degli ordini professionali[6] sia da parte della comunità scientifica[7], cosicché, ad esempio, la Conferenza delle autorità indipendenti federali e regionali per la tutela dei dati personali chiede che il procedimento legislativo venga immediatamente bloccato[8].

Questo contributo – volutamente critico[9] – si muove nella stessa direzione, ma ciò che si sostiene non è tanto la necessità di fermare la proposta, quanto una sua sostanziale revisione.

2. Presa di posizione rispetto alla proposta

2.1. Elaborazione deficitaria dal punto di vista dello stato di diritto

Nonostante tutte le critiche, va subito detto che la proposta persegue uno scopo legittimo. Infatti, l'accesso immediato ai dati memorizzati nel *cloud* sta diventando sempre più importante per garantire una giustizia penale efficace ed equa in un mondo sempre più digitalizzato[10].

Il legislatore europeo con il progetto *E-Evidence* si è trovato e si trova ad affrontare sfide importanti, avendo dovuto e dovendo tuttora prendere in considerazione interessi molteplici e solitamente tra loro in conflitto. Per fare solo alcuni esempi: l'interesse all'esercizio dell'azione penale; la tutela (dei dati) degli accusati e soprattutto dei soggetti meritevoli di peculiare protezione (avvocati, giornalisti, dissidenti politici, ecc.); interessi statali (ad. es. degli stati nel cui territorio sono conservati i dati richiesti); e, non da ultimo, gli

[2] Proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale: si v. il documento del Consiglio 15292/18 del 12.12.2018 (in seguito: PRO-E). I supplementi si trovano in: documento del Consiglio 9365/19 del 17.5.2019. Su questo, tuttavia, non si dirà di più.
[3] Parlamento europeo, Dossier LIBE/8/12854.
[4] Cfr. BR-Drs. 215/1/18.
[5] Si vedano le risposte del governo federale ad una interrogazione in BT-Drs. 19/5207, nonché le riserve espresse rispetto alla PRO-E.
[6] Si v., ad esempio, DAV, SN 42/2018; BRAK, SN 28/2018; DRB, SN 6/18.
[7] D. BRODOWSKI, *Daten in der Cloud – Zugang für Strafverfolger aller Staaten?*, in *NJW-aktuell*, 2018, p. 19; C. BURCHARD, *Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 1*, in *ZIS*, 2018, p. 190; C. BURCHARD, *Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 2*, in *ZIS*, 2018, p. 249; H. NEUHAUS, *Grenzenloser Zugriff auf Providerdaten – Aber wie?*, in *DRiZ*, 2019, p. 120; P. SCHAAR, *E-Evidence: Das europäische Gegenstück zum CLOUD Act*, in *MMR*, 2018, p. 705; V. MITSILEGAS, *The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence*, in *Maastricht Journal of European and Comparative Law*, 2018, p. 263.
[8] Decisione della Conferenza delle autorità indipendenti federali e regionali per la tutela dei dati personali del 7 novembre 2018, p. 2.
[9] Per una trattazione più ampia si v. C. BURCHARD, *Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 1*, cit., p. 190; C. BURCHARD, *Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 2*, cit., p. 249.
[10] Un'altra questione è se vi sia effettivamente la necessità di procedere con un regolamento. Sul punto, per quanto a mia conoscenza, non esiste un'indagine indipendente che vada oltre le affermazioni aneddotiche.

interessi degli ISP[11] a loro volta molto diversi a seconda delle dimensioni dell'impresa e della politica di tutela dei dati personali adottata. A ciò si aggiunge la criticità, nell'ottica del rispetto della *rule of law*, dell'attuale disciplina normativa e soprattutto della prassi applicativa relativa all'accesso ai dati salvati nel *cloud*, poiché tali accessi avvengono sfruttando "aree grigie" dal punto di vista giuridico e attraverso una cooperazione informale[12] con gli ISP, quasi di natura privatistica. Inoltre, tutto questo avviene su larga scala: per fare un solo esempio, in Germania le autorità giudiziarie e quelle preposte alla tutela della sicurezza nazionale richiedono ogni anno l'accesso ai dati di decine di migliaia di utenti o account. Questo dimostra la notevole rilevanza pratica del tema.

Pur tenendo in considerazione tutto ciò, non si deve dimenticare che nessun fine legittimo, nessuna necessità politico-criminale e nemmeno l'esigenza di superare l'attuale situazione di criticità riguardo al rispetto della legalità in questo ambito, può di per sé giustificare qualsivoglia intervento normativo. Detto con altre parole, la complessità di rispettare la *rule of law* in questa materia non ne giustifica un rispetto parziale e deficitario!

Così, per evitare un accesso sproporzionato ai dati è opportuno esigere adeguati *checks and balances*.

Questo vale anche e soprattutto se in linea di principio si vuole confidare nel fatto che tali accessi ai dati da parte degli Stati membri dell'Unione europea sono solitamente idonei, necessari e proporzionati[13].

Ciò detto, la proposta convince poco per i seguenti motivi.

Innanzitutto, perché non prevede alcuna armonizzazione del diritto processuale penale che sta alla base. I requisiti specifici per quanto riguarda il sospetto di reato, la richiesta delle prove (poiché i dati sono in possesso di un ISP) e la quantità delle prove (ad es. quale mole di dati può essere richiesta) non si trovano nella proposta[14], così che di fatto quest'ultima favorisce *fishing expeditions* su larga scala.

Inoltre, la proposta affievolisce tutti i controlli transfrontalieri (già gravemente ridotti nella cooperazione internazionale in materia penale) a tutela dei diritti fondamentali e volti ad evitare il verificarsi di abusi, e questo al punto tale da renderli irriconoscibili.

Ancora, lo stato che procede con l'azione penale dovrebbe poter direttamente obbligare gli ISP che sono attivi nel mercato interno e che sono registrati in altri paesi europei a trasferire a livello nazionale i dati contenuti nel *cloud* (estero) da loro controllato e a consegnarli alle autorità nazionali[15]. In tal modo, la tutela, che già prima era garantita solo in misura limitata da parte dello stato richiesto di fornire assistenza giudiziaria, è ulteriormente ridotta.

---

[11] Abbreviazione internazionalmente utilizzata per *Internet Service Provider*, cioè fornitori di servizi internet.

[12] Gli ISP affermano da parte loro che la cooperazione si svolge già in modo formalizzato, poiché loro si sono già dati delle corrispondenti discipline che regolano la cooperazione medesima. Non ci si deve tuttavia dimenticare che questa cooperazione non è disciplinata dal diritto statale e, quindi, è in questo senso informale.

[13] Critico rispetto alla fiducia reciproca come presunto fondamento per il riconoscimento reciproco e in particolare critico rispetto all'affermazione di questa fiducia come principio di diritto costituzionale dell'Unione europea, che quindi può essere impiegato per ponderare la tutela dei diritti fondamentali europei e quindi essere utilizzato per ridurre questi ultimi, si v. ora C. BURCHARD, *Die Konstitutionalisierung der gegenseitigen Anerkennung. Die strafjustizielle Zusammenarbeit in Europa im Lichte des Unionsverfassungsrechts*, Frankfurt a.M., 2019, pp. 483 ss.

[14] L'art. 5, co. 2, PRO-E in collegamento con l'art. 3, co. 2, PRO-E fanno solo riferimento al fatto che, per quanto riguarda gli ordini di produzione, questi devono essere necessari e proporzionati.

[15] L'art. 1, co. 1, PRO-E prevede che un'autorità di uno stato membro possa esigere la produzione e la conservazione delle prove elettroniche e ciò, fondamentalmente, indipendentemente da dove i dati si trovano.

In un certo senso coerentemente a tutto ciò, si prevede che la presa in considerazione delle immunità e dei privilegi è compito primario delle autorità giudiziarie dello stato che esercita l'azione penale. Così, proverbialmente, la capra è fatta giardiniere. A ciò si aggiunga che, se le immunità e i privilegi per i cittadini nazionali (compresi avvocati, giornalisti e dissidenti) dovessero applicarsi solo rispetto ai *server* stranieri, a livello nazionale si sfrutterà "logicamente" la possibilità di ritirarsi in "porti" ove i dati sono protetti in modo più sicuro e quindi proprio su tali *server* stranieri[16].

Ancora, anche il rudimentale meccanismo sostitutivo di controllo da parte degli ISP contro la violazione dei diritti fondamentali e volto a prevenire il verificarsi di abusi, meccanismo che era previsto nel progetto originario della Commissione, è stato successivamente soppresso senza essere sostituito[17].

Da ultimo, occorre evidenziare i deboli obblighi di notifica e i deboli rimedi giuridici a disposizione degli interessati[18].

Diventa quindi chiaro che, nella proposta, gli interessi nazionali e quelli concernenti la sicurezza hanno acquisito un ruolo assolutamente dominante[19].

Così, la proposta mira a realizzare un cambio di paradigma nella giustizia penale transnazionale, sostituendo il classico principio di territorialità con il principio del mercato, al fine di obbligare gli ISP attivi a livello nazionale a fornire dati esteri. In questo modo, il luogo in cui i dati sono conservati non dovrebbe più svolgere alcun ruolo.

Tutto questo è inaccettabile in uno stato di diritto, è impropriamente troppo "rivoluzionario" e, inoltre, è irragionevolmente unilaterale. In altre parole, la proposta è sproporzionata e quindi già contraria al diritto primario o al diritto costituzionale dell'Unione europea, così che non si debba ancora prendere in considerazione l'eventuale strada per Karlsruhe (per violazione del diritto costituzionale tedesco).

2.2. Distante dalla realtà in quanto basato su una differenziazione giuridica superata

Inoltre, la proposta è superata dalla realtà perché non prende atto dei più recenti sviluppi tecnici e delle differenti tipologie di utenti, facendo riferimento a differenziazioni giuridiche superate.

Così, non viene fatta alcuna distinzione tra i diversi modelli di *cloud* (da *shards* fino a *data trusts*)[20], con la conseguenza che gli utenti che archiviano i loro dati "gratuitamente" presso ISP che non promettono una protezione specifica dei medesimi saranno messi su un piano di parità con gli utenti (in particolare commerciali) che, al contrario, sostengono anche

[16] Cfr. in particolare il considerando 35 della proposta di regolamento.
[17] Cfr. art. 9, co. 5, § 2, PRO-E, che nella proposta si trova ancora come testo barrato.
[18] Il considerando 43 della proposta di regolamento stabilisce esplicitamente che gli interessati non devono essere informati dagli ISP e nemmeno, in certi casi, dalle autorità emittenti sul fatto che i loro dati sono stati richiesti. Cfr. anche la nota 38 all'articolo 17 della proposta di regolamento.
[19] In tanto in quanto, eccezionalmente, la proposta imponga requisiti più rigorosi per la cooperazione con gli ISP, è significativo che siano già in corso discussioni sulla possibilità di evitarli attraverso una cooperazione "tradizionale", vale a dire informale, con i medesimi ISP.
[20] Più approfonditamente C. BURCHARD, *Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 2*, cit., p. 249 e ora anche P.M. SCHWARTZ, *Legal Access to the Global Cloud*, in *Columbia Law Review*, 2018, p. 1681; cfr., al contrario, il considerando 17 PRO-E, che parla genericamente di infrastrutture basate sul *cloud*.

costi notevoli proprio in virtù della migliore protezione dei loro dati (garantita dall'ubicazione territoriale dei centri di raccolta). In questo modo non si tiene in considerazione il fatto che i dati contenuti nel *cloud* non sono – come comunemente sostenuto – sempre "volatili"[21], poiché, tutt'al contrario, alcuni modelli di *cloud* si basano sul fatto che i dati devono essere memorizzati "in modo sicuro" in determinati luoghi, come ad esempio, previsto in Germania dalla legge sulla protezione dei dati personali.

In sintesi, in primo luogo, il progetto tratta situazioni diverse in modo irragionevolmente simile (ossia modelli di *cloud* tra loro diversi e differenti comportamenti degli utenti); in secondo luogo, la proposta limita anche i legittimi interessi commerciali di quegli ISP che sono giustamente sempre più spesso ricompensati per la fiducia riposta dai loro clienti nella sicurezza dei loro dati[22].

All'opposto, la proposta perpetua la tradizionale differenziazione per tipo di dati e considera l'accesso ai dati relativi agli abbonati e al traffico (ad esempio, dove è stata consegnata un'e-mail!) come un'intrusione meno significativa rispetto all'accesso ai dati sui contenuti (ad esempio, il contenuto dell'e-mail!)[23]. È evidente come tutto ciò non sia più appropriato ai tempi dei Big Data, proprio perché – ad esempio – l'accumulo dei dati di accesso può essere utilizzato per creare profili di movimento accurati e altamente lesivi dei diritti fondamentali.

2.3. Pregiudizio a legittimi interessi di sicurezza degli Stati membri dell'Unione Europea

Da un lato, la proposta promette un successo nelle indagini assolutamente a breve termine ed è, inoltre, in linea con gli sforzi posti in essere da altri Stati che stanno creando o intendono ottenere l'accesso ai dati in *cloud* extraterritoriali attraverso obblighi unilaterali in capo agli ISP privati (l'esempio più evidente è il *Cloud Act* statunitense[24]). Dall'altro lato, tuttavia, queste "appropriazioni nazionali" dei *cloud* già osservabili a livello mondiale sono a lungo termine in contrasto con gli interessi europei in tema di sicurezza.

Il primo rischio è che si verifichi un'erosione della cooperazione internazionale in materia di sicurezza, cooperazione da cui continuano a dipendere tutti gli stati liberal-democratici per far fronte alle minacce transfrontaliere. A questo proposito, è importante prendere sul serio l'opinione di un *ex* procuratore di alto livello nonché consigliere per la sicurezza nazionale, secondo il quale il crescente spostamento «from multilateral cooperation and toward a go-it-alone unilateralism, diminishing the cooperation of law enforcement and intelligence agencies around the world, [is] worrisome given the critical role cooperation

[21] Cfr. solo COM (2018) 225 definitivo, p. 1 («Internet non conosce confini») e p. 2 («Volatilità delle prove elettroniche») nonché i riferimenti in C. BURCHARD, *Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 2*, cit., p. 249.

[22] Sul punto si v. anche Parlamento europeo, terzo documento di lavoro (A) sulla proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale, 2018/0108 (COD), p. 4.

[23] Cfr. solo l'art. 5, co. 3 e 4, nonché i considerando 23, 30 e 31 della proposta di regolamento.

[24] Si v. solamente S. BILGIC, *Something Old, Something New, and Something Moot: The Privacy Crisis Under the CLOUD Act*, in *Harvard Journal of Law and Technology*, 2018, p. 321; J. DASKAL, *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, in *Stanford Law Review Online*, 2018, p. 9; M. RATH-A. SPIES, *CLOUD Act: Selbst für die Wolken gibt es Grenzen*, in *CCZ*, 2018, p. 229.

plays in tackling modern crossborder crime and cyberthreats – dangers that did not exist, or were not as virulent, decades ago»[25].

Inoltre, la politica estera dell'UE è minacciata dalla condizione di reciprocità. Se le autorità giudiziarie europee possono richiedere agli ISP transnazionali che operano nel mercato interno europeo la fornitura di tutti i dati (anche se sono situati all'estero o riguardano stranieri), perché allora i paesi stranieri non dovrebbero agire negli stessi termini e richiedere agli ISP di fornire dati situati su *server* europei (ad esempio, tedeschi) o riguardanti cittadini europei (ad esempio, tedeschi)? Così, si avverte che si avrà una situazione in cui «[i]f every country asserts extraterritorial jurisdiction [....] then everybody gets everybody's data»[26], situazione che in ultima analisi promuove un aggiramento globale delle norme europee in materia di protezione dei dati.

Infine, se i dati nel *cloud* non sono più tutelati dall'accesso unilaterale da parte delle autorità giudiziarie di tutti i paesi, anche gli utenti medi saranno sempre più spinti ad utilizzare concetti "alternativi", cyber-anarchici, di protezione dei dati. Retoricamente ci si deve chiedere se è davvero nell'interesse delle autorità giudiziarie europee che gli utenti medi in futuro stiano più attenti alla produzione di dati e comincino a criptarli "più efficacemente"[27].

3. Possibili soluzioni

Di seguito sono illustrati i possibili approcci che potrebbero essere adottati per risolvere le criticità sopra individuate.

3.1. Scelta della base giuridica

Una disciplina sull'accesso ai dati sui *cloud* stranieri che sia conforme al diritto costituzionale europeo e che sia accettabile dal punto di vista dello stato di diritto deve innanzitutto riconoscere che si tratterebbe dell'introduzione di una misura processual-penale obbligatoria (nuova per molti Stati membri). Così, in termini di competenza giuridica, deve se mai essere impiegata la base giuridica fornita dall'art. 82, co. 2, TFUE[28], che riguarda l'armonizzazione del diritto processual-penale degli Stati membri. Al contrario, il ricorso – così come previsto nella proposta – all'art. 82, co. 1, TFUE (cooperazione giudiziaria in materia penale, in particolare riconoscimento reciproco), è una base giuridica artificiosa nella migliore delle ipotesi e probabilmente scelta strategicamente e che, pertanto, deve essere abbandonata[29].

3.2. Disciplina processual-penale

[25] Riferimenti in C. BURCHARD, *Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 2*, cit., p. 255, n. 48.
[26] Così, John Frank, Vicepresidente Microsoft per gli affari governativi UE. Riportato da J. FIORETTI, *Europe seeks power to seize overseas data in challenge to tech giants*, Reuters Business News, 26.2.2018.
[27] Cfr. anche N.M. RICHARDS-W. HARTZOG, *Privacy's Trust Gap*, in *Yale Law Journal*, 2017, p. 1196.
[28] Compreso il cosiddetto "freno di emergenza" di cui all'art. 82, co. 3, TFUE.
[29] Critico rispetto all'art. 82, co. 1, TFUE anche Parlamento europeo, Dossier LIBE/8/12854, secondo documento di lavoro (A), 6.2.2019, pp. 7 ss.; DAV, SN 42/2018, p. 7; BRAK, SN 28/2018, p. 3.

Un'armonizzazione del diritto processual-penale degli Stati membri presuppone norme dettagliate – qui descrivibili solo in termini molto vaghi – con riferimento ai requisiti tecnici, processuali, di ricorso e sostanziali sulla base dei quali gli ISP attivi sul territorio nazionale possono essere obbligati a fornire dati conservati all'estero (ad es. con riferimento al grado di sospetto, alla gravità del reato, ai requisiti per l'autorità emittente, in particolare per quanto riguarda l'autorizzazione tecnica, nonché con riferimento al volume dei dati richiesti). Solo in questo modo è possibile esaminare sia la proporzionalità in astratto dell'atto giuridico sia l'ammissibilità e la proporzionalità in concreto delle singole richieste di dati.

Inoltre, poiché l'accesso ai dati contenuti nel *cloud* avviene solitamente in segreto, devono essere stabilite regole generali precise con riferimento ai requisiti e alla portata della disciplina[30]. Ancora, occorre chiarire le questioni del divieto di prova, del divieto di utilizzo, nonché della tutela giuridica.

Particolare attenzione deve essere prestata alle persone e ai gruppi vulnerabili (clero, giornalisti, avvocati, dissidenti, ecc.). I loro dati, infatti, dovrebbero poter essere consultati (se proprio) solo sulla base di particolari condizioni che devono essere disciplinate dall'atto giuridico.

Inoltre, le difficoltà dal punto di vista della disciplina processual-penale derivano dal fatto che spesso non è possibile determinare *ex ante* la portata dell'intromissione provocata dalla richiesta dei dati. Il riferimento a classificazioni astratte (come i contenuti o i dati sul traffico) è diventato tecnicamente obsoleto (cfr. *supra* 2.2). Figurativamente, l'accesso a uno *smiley*, dopo tutto un contenuto di un SMS, determina un'intromissione di portata meno significativa rispetto all'accesso ai dati sul traffico, ovvero dove e quando questo SMS è stato inviato. E l'accesso a dati diversi, di per se dati non particolarmente rilevanti dal punto di vista dei diritti fondamentali, può determinare una significativa violazione dei medesimi diritti fondamentali, perché una sommatoria di dati ha un "peso" più elevato rispetto alla somma di parti di dati.

Così, per tener conto di ciò, oltre ai requisiti *ex ante*, è necessario prevedere e regolamentare anche una costante valutazione generale, con conseguenze processual-penali in caso di superamento di determinate soglie di intromissione (ad esempio, se attraverso i metadati è possibile ricavare un dettagliato profilo dei movimenti allora vi è l'esigenza di una successiva approvazione giudiziaria e di regole separate per l'utilizzo e l'elaborazione).

Inoltre, gli interessati devono essere informati in modo esauriente[31] circa l'accesso (al più tardi) quando le indagini sono di fatto concluse, non da ultimo anche per consentire un controllo giuridico oggettivo, ad esempio dal punto di vista dell'interesse pubblico a proseguire l'indagine. Non solo, tutte le persone interessate dall'accesso ai dati devono essere informate, comprese quelle contro le quali non sono in corso ulteriori indagini, quelle contro le quali non è stato possibile accertare l'esistenza di dati (utilizzabili) o che sono state solo incidentalmente interessate. Solo in questo modo si può porre un freno ad un (pericoloso) accesso su larga scala ai dati sulla base di motivazioni "campate in aria".

[30] Cfr. D. BRODOWSKI, *Verdeckte technische Überwachungsmaßnahmen im Polizei- und Strafverfahrensrecht. Zur rechtsstaatlichen und rechtspraktischen Notwendigkeit eines einheitlichen operativen Ermittlungsrechts*, Tübingen, 2016, p. 497.

[31] In questo senso anche DAV, SN 42/2018, pp. 10 ss.; Parlamento europeo, Dossier LIBE/8/12854, sesto documento di lavoro (A), 11.3.2019, p. 3.

Ma, come sempre accade quando si introduce un obbligo in capo ai privati (in questo caso, ISP privati che devono trasferire dall'estero i dati e renderli disponibili), anche i loro interessi devono essere presi in adeguata considerazione.

3.3. Disciplina intergovernativa

In questo modo sono però delineati "solamente" i requisiti processual-penali nazionali.

Va quindi aggiunto che, se si vuole mantenere il modello normativo dell'obbligo diretto in capo agli ISP di fornire dati stranieri, deve essere concessa una sorta di "compensazione" per l'attraversamento delle frontiere nel caso di accesso ai dati[32]. Questo può e deve essere basato sulla tipologia di utente e sul modello di *cloud* in questione (si v. *supra* 2.2):

- se vi è stato un sufficiente (!) chiarimento agli utenti e una corrispondente prassi di diritto internazionale, nel caso di accesso ai dati *cloud* salvati fisicamente in una località che, con la conoscenza e la volontà dell'utente, è scelta casualmente[33], si può considerare superflua una notifica allo stato in cui i dati sono effettivamente conservati;

- se, invece, non sono state fornite informazioni sufficienti e se i dati riguardano cittadini stranieri, è necessario informare il paese d'origine delle persone interessate. Infatti, solo questo paese avrà un effettivo interesse ad assicurare la tutela dei suoi cittadini nel *World Wide Web*;

- da ultimo, la procedura è di nuovo diversa se i dati sono memorizzati con la conoscenza e la volontà dell'utente in un luogo specifico, ad esempio in un luogo con un livello particolarmente elevato di protezione dei dati. In questo caso, anche lo stato in cui si trovano i dati deve essere informato, perché si può presumere che quest'ultimo abbia un interesse (anche economico!) a garantire uno "scudo" per la protezione dei dati rispetto all'esterno.

Inoltre, i requisiti e le conseguenze di una tale notifica devono essere determinati in dettaglio e in ogni caso, lo stato notificato deve avere la possibilità di "recuperare" efficacemente i dati prelevati – ad esempio in caso di violazione dell'ordine pubblico europeo –, ossia di impedire che i dati già forniti da un ISP vengano utilizzati nonostante l'obiezione dello stato notificato[34].

A tal fine, può diventare necessario erigere nello stato che riceve i dati una sorta di "muraglia cinese" tra il destinatario nazionale dei dati e l'organo che esercita l'azione penale. Da notare che, anche in questo caso, sarebbe necessario un dettagliato atto giuridico europeo.

3.4. Nessuna rinuncia alla cooperazione internazionale in materia di sicurezza

[32] Come ha dichiarato in un altro contesto il BVerfGE 142, 234, in NJOZ, 2017, 599, marginale 34 con riferimento al diritto costituzionale tedesco: «poiché il potere dello stato all'estero è soggetto solo ai suoi propri vincoli giuridici, il legislatore tedesco deve garantire soprattutto nel caso di trasferimento di dati personali ad autorità estere che i limiti sostanziali previsti a livello costituzionale alla raccolta e al trattamento dei dati personali non vengano nella loro sostanza superati e che, in particolare, i principi fondamentali dello stato di diritto non siano violati. In nessun caso lo Stato può contribuire a violazioni della dignità umana».

[33] Ad esempio, se e in quanto il luogo di memorizzazione è determinato attraverso algoritmi che prestano attenzione solo all'efficacia e all'efficienza della memorizzazione stessa.

[34] Su questa problematica si v. anche Parlamento europeo, Dossier LIBE/8/12854, quinto documento di lavoro (C), 8.3.2019, p. 5.

Anche se è forse illusorio nell'attuale situazione geopolitica ricordare i vantaggi della cooperazione – nel senso letterale del termine – internazionale in materia di sicurezza, l'UE dovrebbe finalmente attivarsi per regolamentare in modo uniforme a livello internazionale l'accesso per ragioni processual-penali ai dati contenuti nel *cloud*.

Le risorse attualmente impiegate a livello mondiale in nuovi atti giuridici unilaterali potrebbero anche essere investite, ad esempio, nel funzionale sviluppo di un sistema di assistenza giudiziaria autentico e affidabile, in cui i pubblici ministeri di tutto il mondo lavorano insieme per controllare la criminalità transfrontaliera e per respingere le richieste di cooperazione che pongono interrogativi circa il rispetto delle garanzie fondamentali dello stato di diritto.

Gli esempi pratici dimostrano che l'assistenza giudiziaria reciproca può svolgersi al tempo stesso in modo rapido ed efficiente e in modo tale da garantire i requisiti minimi della *rule of law*. Ciò è possibile, in particolare, quando c'è la volontà di cooperare "di qua e di là". La rinuncia proclamata da tutte le parti alla cooperazione giudiziaria è quindi "semplicemente" fuori luogo e, pertanto, una nuova e rivoluzionaria regolamentazione dell'accesso ai dati nei *cloud* stranieri è "semplicemente" inappropriata.

Tuttavia, quanto detto potrebbe attualmente rimanere un mero auspicio.

4. Riflessioni conclusive

Nel complesso, la proposta di regolamento europeo sulle prove elettroniche è discutibile sotto più punti di vista, peraltro qui solo brevemente descritti. Quindi, si può solo sperare che il dialogo a tre con (l'appena eletto) Parlamento europeo porti all'elaborazione di una disciplina che sia al tempo stesso equilibrata in termini di rispetto delle garanzie, che rifletta correttamente la realtà e che sia pensata anche in una prospettiva di lungo termine, cosicché la criminalità dell'era digitale possa essere affrontata efficacemente e con modalità conformi allo stato di diritto.