FONDAZIONE OCCORSIO

Atti del workshop

INTELLIGENZA ARTIFICIALE E GIURISDIZIONE PENALE

Universitas Mercatorum
Roma, Piazza Mattei, 10
19 novembre 2021

FONDAZIONE VITTORIO OCCORSIO

INDICE

Illustrazione della regolamentazione europea sulla *Mutual Legal Assistance* (MLA) nel *cyberspace*

di Beatrice Fragasso
Dottoranda di ricerca in Diritto penale, Università degli Studi di Milano

Nella relazione che segue cercherò di rilevare quali sono le prospettive della normativa europea ed internazionale in materia di giurisdizione e di acquisizione delle prove elettroniche.

I problemi inerenti all'esercizio della giurisdizione nel *cyberspace* non sono una novità e risalgono agli albori di internet: tali problemi sono tuttavia oggi esacerbati dall'incremento di rapidità del flusso di dati, dall'evoluzione degli strumenti tecnologici virtuali, ma soprattutto dalla *pervasività* dello spazio virtuale.

Se infatti nel 2001 – quando è stata siglata la Convenzione di Budapest[7] – l'obiettivo era di garantire un'adeguata prevenzione e repressione di un piccolo nucleo di reati informatici – riconducibili a nove categorie – oggi non solo le condotte offensive *online* si sono moltiplicate, ma si può dire che praticamente tutti i reati lasciano tracce nel mondo virtuale, ponendo agli organi investigativi il problema di acquisire prove decisive in uno spazio deterritorializzato, sul quale spesso non esercitano la giurisdizione.

In materia di sicurezza informatica, vi sono due piani distinti che possono entrare in gioco: da un lato, i rapporti tra stati sovrani, con i cyberattacchi che possono configurarsi come veri e propri atti di guerra e di violazione della sovranità statale; dall'altro lato, la commissione di reati nello spazio virtuale.

L'identificazione dell'ambito di riferimento è di fondamentale importanza, poiché implica l'applicazione di un *corpus* normativo in luogo dell'altro. In un caso, infatti, si farà ricorso al Diritto internazionale, ed eventualmente allo *ius in bello*. Nel secondo caso, si utilizzeranno gli ordinari strumenti giurisdizionali del processo penale.

Va tra l'altro rilevato che nel concreto sembra sempre più complesso distinguere i due piani. Il rapporto tra cybercriminali e organi governativi di alcuni paesi è ormai sotto gli occhi di tutti. Tuttavia, sia che si tratti di criminali comuni, sia che si tratti di *hacker* al soldo dei Governi, si pone un problema centrale, che è quello dell'attribuibilità e, dunque, dell'accesso alla prova elettronica. Come individuare l'autore del fatto illecito, in un contesto in cui – approfittando della volatilità e frammentarietà dei dati – i criminali possono far rapidamente sparire le proprie tracce?

Ecco che allora la comunità internazionale e l'Unione Europea – e prima ancora gli Stati Uniti – si stanno muovendo lungo una chiara direttrice, che è quella della collaborazione diretta con gli *Internet Service Provider*.

---

[7] Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica, aperta alla ratifica il 23 novembre 2001.

Prima di concentrarci sulle proposte che sono in corso di discussione in ambito europeo e internazionale, può essere utile porre l'accento sull'attuale disciplina dell'accesso ai dati e sulle criticità che sono state riscontrate. Oggi l'accesso ai dati è regolato dai meccanismi di cooperazione giudiziaria, previsti sia dalla Convenzione di Budapest (artt. 23 e 25), sia da fonti dell'UE (tra le tante, possiamo limitarci a ricordare la Direttiva del 2014 sull'Ordine europeo di indagine[8]), nonché da accordi bilaterali sulla mutua assistenza giudiziaria tra l'Unione e gli Stati terzi, come quello con gli Stati Uniti d'America[9] e con il Giappone[10].

Nella prassi, tuttavia, l'acquisizione di prove digitali ha incontrato alcune peculiari criticità. In primo luogo, la lentezza: in un contesto globalizzato in cui i *cyberattacks* sono all'ordine del giorno, i procedimenti di MLA risultano lenti e farraginosi, richiedendo spesso alcuni mesi per la loro implementazione[11]. Le norme che regolano questi meccanismi sono state concepite per le prove fisiche, e prevedono tempistiche di trasmissione inadatte alla velocità con cui le prove digitali si muovono nella rete e possono trasmigrare da uno Stato ad un altro.

In secondo luogo, i meccanismi di assistenza giudiziaria presuppongono un unico Stato di esecuzione. La dispersione delle prove digitali, tuttavia, spesso porta alla moltiplicazione delle giurisdizioni coinvolte. Qual è, allora lo Stato di esecuzione? Lo Stato in cui opera o ha la sede legale il *service provider* che ha accesso alle prove? Oppure lo Stato in cui si trova il *server* dove si trovano le prove, magari diverso dallo Stato del *provider*[12]? E in quest'ultimo caso, come effettuare la scelta qualora, come spesso accade

---

[8] Direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale.

[9] Accordo sulla mutua assistenza giudiziaria tra l'Unione europea e gli Stati Uniti d'America (GU L 181 del 19.7.2003).

[10] Accordo tra l'Unione europea e il Giappone relativo all'assistenza giudiziaria in materia penale (GU L 39 del 12.2.2010).

[11] CYBERCRIME CONVENTION COMMITTEE (T-CY), *T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime adopted by the T-CY at its 12th Plenary (2–3 December 2014)*, disponibile sul sito del Consiglio d'Europa; vd. anche l'*impact assessment* all'*E-evidence package*, *Commission staff working document impact assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings* – SWD/2018/118 final, *passim*; B. KOOPS – M. GOODWIN, *Cyberspace, the cloud, and cross-border criminal investigation*, *in Tilburg Law School Research Paper No. 5/2016*; T. CHRISTAKIS – F. TERPAN, *EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options*, in *International Data Privacy Law*, 2021, Vol. 11, No. 2; nella letteratura italiana vd. M. DANIELE, *L'acquisizione delle prove digitali dai* service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Rev. Bras. de Direito Processual Penal*, vol. 5, n. 3, 2019, p. 1280; 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 *Dir. pen. cont.*, 5/2018, p. 281.

[12] Come accaduto, ad esempio, nel noto caso deciso dalla Corte Suprema, *United States v. Microsoft Corp., 584 U.S (2018)*, in cui l'autorità giudiziaria statunitense aveva chiesto a Microsoft, azienda statunitense, alcuni dati reperibili in un server situato in Irlanda. In particolare, in quella vicenda, Microsoft aveva rifiutato di fornire l'e-mail di un cittadino americano – conservata in un server in Irlanda – dopo aver ricevuto un mandato dall'FBI ai sensi dello *Stored Communications Act* (*section 703*). Il rifiuto aveva aperto una controversia legale, poiché Microsoft sosteneva che l'SCA non copriva i dati conservati al di fuori degli Stati

per ragioni economiche od organizzative, le prove vengano fatte costantemente circolare fra *server* situati in Stati diversi?

In assenza di soluzioni internazionali condivise, ad oggi gli accessi avvengono attraverso una cooperazione informale con i fornitori di servizi, quasi di natura privatistica[13]. Ogni anno, le autorità giudiziarie e le agenzie di *intelligence* dei paesi europei richiedono l'accesso a decine di migliaia di dati su utenti e *account*. In base ad un recente studio condotto da *Eurojust*[14], risulta ad esempio che nel 2020 le richieste inviate dalla Germania agli *Internet Service Provider* (quali, ad esempio, Apple, Facebook. Google e Twitter) siano state 63.561; la Francia ne ha invece inoltrate 43.252 e l'Italia 10.699.

L'inefficienza del sistema emerge plasticamente dall'*Impact Assessment* che ha accompagnato la presentazione delle proposte europee in tema di prova elettronica[15], dal quale si evincono tre dati di rilievo:

(i) più della metà delle indagini effettuate in UE comprende una richiesta di accesso transfrontaliero alle *e-evidence*[16];

(ii) meno della metà delle richieste ai fornitori di servizi vengono soddisfatte[17];

(iii) quasi due terzi dei reati che comportano un accesso transfrontaliero alle prove elettroniche – con le attuali regole europee – non possono essere efficacemente indagati o perseguiti[18].

È proprio l'obiettivo di facilitare l'acquisizione della prova elettronica ad aver ispirato l'elaborazione di alcune proposte normative: il Regolamento e la Direttiva che compongono l'*E-Evidence Package*[19] ed il Secondo protocollo addizionale alla

---

Uniti e che l'FBI avrebbe potuto beneficiare soltanto di meccanismi di cooperazione giudiziaria. Approvato il *Cloud Act*, il governo federale ha ottenuto un nuovo mandato conforme al *Cloud Act*, che sostituiva il precedente. La Corte Suprema ha dunque rigettato il ricorso dichiarando l'irrilevanza della questione proposta.

[13] Così C. BUCHARD, *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*, in *Eurojus*, 2/2020, p. 201; vd. anche 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*, 2018, Vol. 9(3), *passim*; I. WALDEN, *Law Enforcement Access to Data in Clouds*, in C. Millard (ed.) *Cloud Computing Law*, Oxford University Press, p. 283 ss.

[14] SIRIUS EU Digital Evidence Situation Report, 3d annual report, 2021, p. 55, disponibile sul sito di *Eurojust*. Il report si riferisce all'anno 2020.

[15] *Proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale* – COM/2018/225 final - 2018/0108 (COD) e *Proposta di direttiva del Parlamento europeo e del Consiglio recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali* – COM/2018/226 final - 2018/0107 (COD); per l'*impact assessment* vd. *Commission staff working document* – SWD/2018/118 final, cit.

[16] *Commission staff working document* – SWD/2018/118 final, cit., p. 14.

[17] *Ibidem*, p. 15.

[18] *Ibidem*, p. 17.

[19] *Proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, cit.; *Proposta di direttiva recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali*, cit.

Convenzione di Budapest[20]. Questi strumenti si muovono tutti nella medesima direzione, che è quella di garantire agli Stati parte una procedura legale per accedere alle prove elettroniche mediante una richiesta diretta al fornitore di servizi; senza, dunque, alcun coinvolgimento dell'autorità giudiziaria del paese ospitante. In particolare, la proposta di Regolamento dell'UE sull'*E-evidence* prevede due tipologie di richieste: l'ordine di produzione, mirato alla trasmissione dei dati, che deve essere adempiuto nel termine di dieci giorni (sei ore, nei casi di emergenza)[21]; l'ordine di conservazione, finalizzato invece alla custodia dei dati in vista di una successiva richiesta di produzione[22]. In caso di inadempienza, i *provider* possono essere sottoposti a sanzioni pecuniarie[23].

Gli elementi di novità sono molteplici, e corrispondono ad altrettante linee di tendenza della regolazione del *cyberspace* a livello globale.

Innanzitutto, un primo fondamentale elemento di novità consiste nell'obbligo per i fornitori che offrono i loro servizi nell'Unione Europea di designare un rappresentante legale per la ricezione delle richieste e per l'applicazione della normativa[24]. Si assiste dunque ad un tentativo di ri-territorializzare la giurisdizione, prendendo atto che uno dei maggiori ostacoli all'ottenimento delle prove elettroniche, fino ad ora, è consistito nel rifiuto dei *providers* di fornire dati localizzati fuori dalla giurisdizione dello stato richiedente. La stessa dott.ssa Nunzia Ciardi – vicedirettrice dell'Agenzia per la Cybersicurezza Nazionale e per anni a capo della Polizia Postale – nel precedente incontro organizzato dalla Fondazione Occorsio raccontava come, ad oggi, sia di fatto impossibile accedere ai dati detenuti da *Telegram*, dato che la società non rende nemmeno nota la sede presso la quale effettuare le notifiche.

In secondo luogo, vi è un superamento della logica centralizzata fondata sulla necessaria interlocuzione tra le autorità dello stato di emissione e dello stato di esecuzione.

Si va dunque verso una disintermediazione, che, se da un lato permetterà un *enforcement* più rapido ed efficiente, dall'altro costituisce un ulteriore capitolo del crescente ruolo assunto dalle società private nella tutela dei diritti fondamentali[25].

---

[20] *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, CM (2021)57-final.

[21] *Proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, cit., artt. 5 e 9.

[22] *Proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, cit., art. 6.

[23] *Proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, cit., art. 13.

[24] *Proposta di direttiva recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali*, cit.

[25] Il dibattito in letteratura è molto ampio. Si vedano, per tutti, 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; M. DANIELE, *L'acquisizione delle prove digitali dai* service provider, cit.; A. ROSANÒ, *La "privatizzazione" nello spazio di libertà, sicurezza e giustizia: tre esempi per una tendenza*, in *Il Diritto dell'Unione europea*, 2020, p.179 ss.

Una volta ricevuto l'ordine, infatti, i *providers* dovranno controllare l'eseguibilità degli ordini, sulla base di criteri non molto diversi da quelli ordinariamente utilizzati dalle autorità giudiziarie chiamate ad eseguire le rogatorie e gli Ordini europei di indagine. Tra i criteri vi sono, ad esempio, la verifica circa la manifesta violazione della Carta di Nizza o la manifesta arbitrarietà della richiesta[26].

Una disposizione non dissimile si riscontra tra l'altro nel *CLOUD Act* del 2018[27], l'omologo statunitense del regolamento europeo.

La politica di attribuzione ai fornitori di servizi online di poteri di (*soft*) *enforcement* non è, d'altra parte, un fenomeno nuovo, specialmente per quanto concerne il controllo sui contenuti pubblicati dagli utenti sui *social network*[28]: un compito molto delicato – quello di stabilire cosa è lecito e cosa no, cosa costituisce legittima manifestazione del pensiero e cosa, invece, rappresenta un pericolo per la pubblica sicurezza o una lesione della dignità personale – che corrisponde ad una funzione di bilanciamento di diritti tradizionalmente svolta dagli organi giurisdizionali.

In ogni caso, la via del dialogo diretto con i fornitori di servizi sembra oggi il modello privilegiato in materia di accesso alle prove elettroniche. Il Secondo Protocollo alla Convenzione di Budapest propone uno strumento assimilabile[29] e sono in corso negoziazioni tra Unione Europea e Stati Uniti per garantire meccanismi analoghi per l'accesso transfrontaliero ai dati[30].

Non può essere trascurato, tuttavia, che anche il rapporto diretto con i *service provider* nulla può in relazione ai sistemi di criptazione *end-to-end*, quali WhatsApp, Telegram e Signal.

---

[26] *Proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, cit., art. 14, par. 4 (per l'ordine europeo di produzione) e per 5 (per l'ordine europeo di conservazione).

[27] *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act), H.R.4943 - 115th Congress (2017-2018), disponibile sul sito del Congresso; vd. (2) MOTIONS TO QUASH OR MODIFY: «*A provider of electronic communication service to the public or remote computing service, including a foreign electronic communication service or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes* […] *(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government*».

[28] Per una ricognizione dei problemi in materia vd. K. KAESLING, *Privatising Law Enforcement in Social Networks: A Comparative Model Analysis*, in *Erasmus Law Review*, 11, 2018, p. 151 ss.; E. COCHE, *Privatised Enforcement and the Right to Freedom of Expression in a World Confronted With Terrorism Propaganda Online*, in *Internet Policy Review* 7(4), 2018; M.K. LAND, *Against Privatized Censorship: Proposals for Responsible Delegation*, in *Virginia Journal of International Law*, vol. 60-2, 2020, p. 363 ss.

[29] *Second Additional Protocol to the Convention on Cybercrime*, cit., *Section 2 – Procedures enhancing direct co-operation with providers and entities in other Parties*.

[30] Vd. *Decisione del consiglio che autorizza l'avvio di negoziati in vista della conclusione di un accordo tra l'Unione europea e gli Stati Uniti d'America sull'accesso transfrontaliero alle prove elettroniche per la cooperazione giudiziaria in materia penale*, 21 maggio 2019, 9114/19; vd. anche l'*Addendum to the Recommendation for a COUNCIL DECISION authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters*, 27 maggio 2019, 6102/19 ADD 1; per una panoramica sui contenuti delle negoziazioni vd. T. CHRISTAKIS – F. TERPAN, *EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options*, in *International Data Privacy Law*, 2021, Vol. 11, No. 2, 2021.

In questi casi, infatti, nemmeno il fornitore del servizio può accedere alle chat, poiché le chiavi di decodificazione del messaggio criptato appartengono soltanto al *device* del destinatario del messaggio. Anche qualora, dunque, le autorità giudiziarie riuscissero ad avere accesso al dato, questo sarebbe illeggibile.

La questione è ovviamente legata alla sempre più diffusa consapevolezza dell'opinione pubblica in ordine alla tutela dei dati personali, ma in realtà ha a che fare anche e soprattutto con profili di sicurezza informatica.

Come già nel 2016 affermavano i vertici di Apple nel rifiutare la richiesta dell'FBI di sbloccare l'Iphone di uno dei responsabili dell'attentato di San Bernardino, sviluppare una *backdoor* può mettere a repentaglio la sicurezza informatica di tutti gli utenti e, in quel caso, avrebbe potuto creare un pericoloso precedente legale. Una volta creata una crepa nel sistema, questa può essere infatti facilmente aggredibile da qualsiasi criminale informatico.

Le stesse motivazioni sono state fornite da Telegram per negare al Governo russo le chiavi per decrittare la chat degli organizzatori dell'attentato alla metro di San Pietroburgo del 2017.

La risposta delle autorità, in quel caso, non si è fatta attendere, e l'*app* di Telegram è stata bloccata sull'intero territorio russo[31]. Il blocco è stato tuttavia aggirato facilmente e il 95% degli utenti ha continuato a collegarsi al servizio di messaggistica, grazie a sistemi di VPN facilmente accessibili[32]. Tra l'altro, l'anno scorso, le autorità russe sono tornate sui propri passi, togliendo il blocco su Telegram, senza tuttavia aver ottenuto – quantomeno secondo quanto emerge dalle dichiarazioni ufficiali della società – alcun passo indietro sui temi della *privacy*[33].

È proprio alla luce di questo rapporto contrastato della Russia con le principali piattaforme *online* (non solo Telegram, ma anche Facebook, Youtube, Linkedin) che va letta la proposta di Convenzione contro il *Cybercrime* presentata quest'anno dalla Russia alle Nazioni Unite[34]. Ci sono diversi aspetti che preoccupano nella proposta, che sono già stati evidenziati dalle ONG e dai ricercatori che si occupano di diritti civili e di diritti digitali, e che puntano alla trasposizione nello spazio virtuale di una concezione autoritaria del rapporto tra cittadini ed autorità[35].

Due esempi:

---

[31] Vd. *Telegram, la Russia inizia a bloccare la app in tutto il Paese*, in *Corriere della Sera online*, a cura della Redazione, 16 aprile 2018.

[32] Vd. M. EDWARDS – V. LO BARCO, *Nonostante il divieto, Telegram sopravvive in Russia - ma per quanto tempo?*, in *Global Voices*, 20 novembre 2020.

[33] Reuters staff, *Russia lifts ban on Telegram messaging app after failing to block it*, in *Reuters*, 18 giugno 2020.

[34] *United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, Draft 29 giugno 2021 (unofficial translation), disponibile sul sito di *Kommersant*, a questo link: https://www.kommersant.ru/docs/2021/RF_28_July_2021_-_E.pdf.

[35] J. HAKMEH, *Russia's Vision for a Cybercrime Treaty*, in *Directions – Cyber Digital Europe*, 16 settembre 2021; T. CLABURN, *Russia tells UN it wants vast expansion of cybercrime offenses, plus network backdoors, online censorship*, in *The Register*, 3 agosto 2021; *Russia: Proposed UN Cybercrime Convention must uphold free speech*, in *Article 19*, a cura della Redazione, 17 febbraio 2022.

(i) si propone un ampliamento della base per l'estradizione, prevedendo che i ventitre crimini informatici elencati non siano mai considerati "reati politici", per i quali le attuali convenzioni internazionali prevedono l'esenzione da estradizione[36];

(ii) la proposta di Convenzione richiede inoltre ai *provider* di fornire "assistenza tecnica", se richiesti dalle autorità – il che sembra far presagire il tentativo di introdurre *backdoor*, da poter sfruttare nell'ambito di procedimenti penali[37].

A tal proposito, non potrebbe essere più distante la posizione espressa dall'Italia nel *Position Paper* presentato alle Nazioni Unite qualche settimana fa[38], in cui si ribadisce la necessità che i diritti civili trovino il pieno riconoscimento nel *cyberspace*. L'esigenza di prevenire e reprimere l'aggressività dei cybercriminali, dunque, non può giustificare la negazione del diritto di libera manifestazione del pensiero e di riservatezza della corrispondenza.

Io credo che la sfida dei prossimi anni, e anzi dei prossimi decenni, sia proprio quella di mantenere, e anzi di rafforzare, le garanzie dei cittadini nello spazio virtuale – garanzie che troppo spesso, ad oggi, sembrano schiacciate dal peso dalle guerre invisibili tra Stati e dagli interessi delle grandi *corporation* a sfruttare i dati personali dei propri utenti.

[36] *United Nations Convention*, cit., Article 46, par. 4.

[37] *United Nations Convention*, cit., Article 75.

[38] MINISTERO DEGLI AFFARI ESTERI E DELLA COOPERAZIONE INTERNAZIONALE, *Italian Position Paper on 'International Law and Cyberspace'*, disponibile sul sito del Ministero a questo link: https://www.esteri.it/wp-content/uploads/2021/11/Italian-Position-Paper-on-International-Law-and-Cyberspace.pdf.