Archivio Penale
settembre–dicembre 2013 fascicolo 3 anno LXV
ISBN 978-88-548-6177-0
DOI 10.4399/97888548617707
pag. 853–864

Hey! You! Get Off My Cloud!

Accesso autoritativo alle nuvole informatiche e diritto internazionale

Gianpaolo Maria Ruotolo

1. Premessa: oggetto dell'indagine. Con l'espressione *cloud computing* (in italiano spesso resa letteralmente con "nuvola informatica") si fa riferimento al complesso di strumenti tecnici attraverso i quali un utente elabora, usa e archivia, per il tramite di Internet, dati contenuti su computer remoti, cioè da questi non fisicamente raggiungibili, sfruttandone le potenzialità di calcolo e memorizzazione.

Lungi dall'esaurirsi in una mera forma di conservazione di dati, il servizio in questione offre all'utente, generalmente dietro pagamento di un canone, l'opportunità di utilizzare apparecchiature molto avanzate e potenti senza essere costretto a dover investire importanti somme per il loro acquisto né doversi preoccupare della loro manutenzione, essendo sufficiente il possesso di un computer che gli consenta di connettersi a Internet e, per il tramite di quest'ultima, alla sua "nuvola".

Evidenti sono i vantaggi derivanti dal fatto che i dati così archiviati sono sempre raggiungibili dal loro titolare, indipendentemente dal luogo in cui si trova, e che l'eventuale danneggiamento e finanche la distruzione del computer utilizzato per accedervi da remoto non potrà in alcun modo danneggiare i dati stessi, dal momento che i medesimi sono stipati sui *servers* del fornitore del servizio, che, è molto probabile, saranno anche dotati di meccanismi di sicurezza e ridondanza più sofisticati ed efficienti di quelli accessibili al solo utente finale.

Il sistema in parola, peraltro, offre anche la possibilità di consultazione ed elaborazione dei medesimi dati da parte di soggetti diversi, fisicamente situati in luoghi differenti, con evidenti vantaggi riguardo alla loro condivisione e circolazione (si pensi, a mero titolo di esempio, alla possibilità offerta a ogni membro di un gruppo di lavoro di apporre modifiche e revisioni ai dati di un progetto comune, rendendo le stesse immediatamente conoscibili a tutti gli altri membri della medesima *equipe*).

È, peraltro, il caso di chiarire come il *cloud computing* abbia a oggetto prestazioni differenziate, spesso contemporaneamente garantite dal fornitore come "livelli" diversi del servizio complessivamente offerto: le funzioni di

tipo più complesso, infatti, necessitano spesso di quelle di livello inferiore per poter operare efficacemente.

Si distinguono così:

a) il "servizio di infrastruttura" (*Infrastracture as a Service,* IaaS), il livello di base del *clouding*, in cui il fornitore del servizio consente all'utente essenzialmente di poter accedere alle sue strutture *hardware* da remoto, al fine di sfruttarne la potenza di calcolo e di memorizzazione[1];

b) il "servizio di piattaforma" (*Platform as a Service,* PaaS) in cui l'utente utilizza da remoto un pacchetto composto da diversi programmi e librerie che gli consentono di sviluppare applicazioni autonome[2];

c) il "servizio di *software*" (*Software as a Service,* SaaS), il quale si fonda sull'idea che il *software* stesso rappresenti oggigiorno una *commodity*[3] e che, di conseguenza, il medesimo abbia bisogno di essere personalizzato per venire incontro alle esigenze individuali dei singoli utenti[4]. Quest'ultima forma di *cloud computing*, la più evoluta, in ultima analisi, rappresenta una peculiare modalità di distribuzione del *software*, in cui il produttore fa utilizzare ai propri clienti, via Internet, i programmi di cui è proprietario: il SaaS si sostanzia così in un insieme di mezzi, servizi e competenze che spesso permette ai soggetti che ne usufruiscono di esternalizzare elementi del loro sistema informativo, beneficiando dell'abbattimento dei relativi costi[5].

Lo sfruttamento di tutti i servizi appena descritti, se da un lato offre importanti opportunità ai suoi utenti, dall'altro comporta però per questi ultimi anche dei rischi (si pensi, ad esempio, ai problemi derivanti alla continuità operativa in caso d'interruzione del servizio di *clouding*, o a quelli per la riservatezza dei dati archiviati su *servers* remoti) e, ancora sotto il profilo più strettamente giuridico–internazionalistico, pone una serie di quesiti del tutto sconosciuti a un uso più tradizionale del computer e finanche di Internet.

1. Si pensi al caso di *Google Compute Engine*, un servizio che consente ai suoi utenti di eseguire i loro calcoli sulle macchine virtuali Linux ospitate nelle *server farms* di *Google*.

2. È il caso di *Google App Engine*, servizio che permette ai suoi utenti lo sviluppo e l'*hosting* di applicazioni web gestite dai *Google Data Center*.

3. Con l'espressione "*commodity*", come noto, si fa riferimento a quei beni offerti su un mercato, senza differenze qualitative, da diversi operatori; prodotti siffatti, in pratica, hanno caratteristiche identiche indipendentemente da chi li produce, come avviene per il petrolio o il latte.

4. Il concetto in parola costituisce uno sviluppo delle idee contenute nel pioneristico lavoro di O'Reily, *The Open Source Paradigm Shift*, in *oreilly.com/tim/articles/paradigmshift* .

5. In letteratura si veda, da ultimo, Denny, *Survey of Recent Developments in the Law of Cloud Computing and Software as a Service Agreement*, in *The Business Lawyer*, 2010, 237 ss.

Infatti tutti i servizi descritti implicano la memorizzazione dei dati dell'utente in *server farms*[6] che potrebbero essere localizzate per i motivi più disparati (economicità, stato della legislazione nazionale *et similia*) in un Paese diverso sia da quello di appartenenza del fornitore del servizio sia di quello del suo utente finale.

È altamente probabile, peraltro, che la delocalizzazione dei servizi di *cloud* possa assumere connotati ancora più estremi, se solo si pensa che il 28 aprile 2009 il *Patent and Trademark Office* statunitense ha rilasciato, a favore di Google Inc., un brevetto relativo al progetto di una nave/*server farm* alimentata a energia marina[7] da collocarsi in acque internazionali, quindi in un luogo che è addirittura sottratto alla sovranità esclusiva di uno Stato[8].

Il coinvolgimento nelle fattispecie di *cloud computing* di una pluralità di ordinamenti giuridici statali comporta quindi, sotto il profilo privatistico, la necessità di fissare dei criteri in base ai quali individuare il diritto applicabile ai rapporti in parola nonché il giudice competente a dirimere le relative controversie, e, in caso di fatti penalmente rilevanti commessi per il tramite di dati ospitati su un *cloud* o che in qualche modo siano ad essi collegati, quello di individuare quale siano l'autorità inquirente competente e il giudice dotato di giurisdizione. Tra questi ultimi aspetti il presente lavoro si concentrerà, in particolare, sul tema dell'acquisizione forzosa (cioè non autorizzata dal loro titolare) di dati ospitati sui *clouds* al fine di individuare le condizioni in presenza delle quali le autorità di uno Stato possono pretendere di accedere a dati conservati su *clouds* allocati sul territorio di un altro Stato. Si pensi, con riguardo a quest'ultimo aspetto, al caso d'indagini che rendano necessaria l'apprensione di dati e informazioni archiviati su *servers* esteri e in particolare ai problemi che potrebbero insorgere nel caso in cui il Paese di allocazione del *server* non abbia concluso alcun accordo di cooperazione giudiziaria con quello dell'autorità procedente.

2. La competenza ad adottare provvedimenti autoritativi sui dati archiviati nei *clouds* come un problema di diritto penale internazionale. La soluzione ai cennati profili relativi a diritto applicabile e giurisdizione competente a dirimere controversie relative alle obbligazioni che si instaurano tra fruitore e fornitore del servizio — le quali, sia detto per inciso, possono essere sia del tipo c.d. *business to business* (B2B) sia di quello *business*

6. Con tale espressione ("fattoria di *server*") ci si riferisce a una serie di *server*, collocati in un unico ambiente al fine di centralizzare gestione, manutenzione e sicurezza.

7. Il brevetto U.S. Patent Office n. 7, 525, 207 concesso è relativo a un *"water–based data center"* il quale « *includes a floating platform–mounted computer data center comprising a plurality of computing units, a sea–based electrical generator in electrical connection with the plurality of computing units, and one or more sea–water cooling units for providing cooling to the plurality of computing units* ».

8. Sul punto v. Swanson, *Google Sets Sail: Ocean–Based Server Farms and International Law*, in *Connecticut Law Review*, 2011, 709 ss.

to consumer (B2C)[9] — può certamente essere individuata facendo ricorso a norme di diritto internazionale privato, comuni o convenzionali: norme siffatte, come noto, hanno proprio la funzione di tracciare meccanismi e criteri idonei a disciplinare rapporti interprivatistici che siano caratterizzati da elementi di estraneità con un dato ordinamento statale[10].

Meccanismi analoghi, però, non sono replicabili per risolvere i problemi di riparto di giurisdizione in campo penale. È appena il caso di ricordare, infatti, che sebbene le norme "di conflitto" possono riguardare ogni settore dell'ordinamento giuridico e non esclusivamente quello giusprivatistico[11], le caratteristiche del diritto penale e della giurisdizione in quel campo — e in particolare la circostanza che vi vuole *forum* e *jus* inscindibilmente legati — rendono opportuna una trattazione e una elaborazione dogmatica delle relative situazioni di conflitto autonoma rispetto al diritto internazionale privato[12].

Il problema della competenza ad adottare provvedimenti autoritativi sui dati archiviati su *servers* situati all'estero ai fini della loro acquisizione forzosa nell'ambito di un procedimento penale ci pare, quindi, debba essere inquadrato come una ipotesi di situazione di conflitto tra entità statali dotate di autonoma giurisdizione in materia penale, cioè come un problema di diritto penale internazionale.

Come noto, con quest'ultima espressione la dottrina si riferiva tradizionalmente[13] all'insieme delle norme interne con le quali un dato ordinamento nazionale disciplina le fattispecie penalmente rilevanti caratterizzate da elementi di estraneità per un qualche aspetto (come, ad esempio, la cittadinanza

9. Per le definizioni v. Gillies, *Electronic Commerce and International Private Law — A Study of Electronic Consumer Contracts*, Aldershot, Burlington, 2008, p. 15 ss.

10. Sul rapporto tra diritto internazionale pubblico e diritto internazionale privato con riguardo alla disciplina di fattispecie *on line* si vedano Castel, *The Internet In Light Of Traditional Public And Private International Law Principles And Rules Applied In Canada*, in *The Canadian yearbook of international law*, 2001, 3 ss.; Schultz, *Carving Up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface* in *European Journal of International Law,* 2008, 799 ss.; Svantesson, *The Relation between Public International Law and Private International Law in the Internet Context,* Conference Paper presentato alla *Australian Law Teachers' Association Conference*, Luglio 2005, Hamilton, New Zealand, reperibile su *www.svantesson.org*. Per un'analisi della disciplina internazionalprivatistica della Rete, per tutti, v. Bariatti, *Internet — Diritto internazionale privato e processuale*, in *Enc. Giur.,* X, Roma, 2002, p. 1 ss.

11. « *Vi sono, infatti, nel nostro e negli altri ordinamenti, norme di diritto penale e di diritto processuale penale internazionale, di diritto amministrativo internazionale, di diritto tributario internazionale, tutte riconducibili, al pari di quelle di diritto processuale civile internazionale e di diritto privato internazionale, alla nozione lata di diritto internazionale privato* »; Mosconi, Campiglio, *Diritto internazionale privato e processuale, Parte generale e obbligazioni*, 2013, p. 3 ss.

12. Cfr. Treves, *La giurisdizione nel diritto penale internazionale*, Padova, 1973, p. 4 ss.; Caracciolo, *Dal diritto penale internazionale al diritto internazionale penale*.

13. Si occupa per la prima volta del problema in esame, nel 1780, Bentham, *Of the Limits of the Penal Branch of Jurisprudence*, in *An Introduction to the Pinciples of Moral and Legislation*.

del reo o il *locus commissi delicti*)[14]: i limiti del presente lavoro ci impediscono di procedere a un'analisi delle caratteristiche e dello sviluppo che la detta branca del diritto ha avuto, analisi cui si è peraltro già da tempo dedicata la dottrina[15]; possiamo limitarci a ricordare che, allo stato di sviluppo attuale, il diritto penale internazionale risulta essere composto sia, e in misura sempre maggiore, da norme di diritto internazionale sia da disposizioni di diritto interno, le quali hanno ad oggetto la delimitazione delle competenze normative e giurisdizionali penali degli Stati[16]. È anche il caso di ricordare come il diritto penale internazionale vada, poi, tenuto distinto dal diritto internazionale penale, che è invece composto dalle norme di diritto internazionale che hanno ad oggetto la repressione e la punizione dei crimini internazionali degli individui.

Ebbene, occorre premettere che l'ordinamento internazionale non pare contenere norme generali volte al riparto della giurisdizione penale tra i vari membri della Comunità internazionale: norme siffatte, quindi, possono essere contenute — ove siano state concordate — esclusivamente in strumenti pattizi di portata bilaterale o multilaterale o, unilateralmente, in disposizioni di diritto interno.

3. I criteri legittimanti la titolarità statale ad adottare siffatti procedimenti: territorialità, nazionalità del reo, nazionalità della vittima, principio della bandiera, principio dell'interesse leso, universalità. Pur nell'assenza di norme universalmente condivise, però, sia le norme di diritto penale internazionale comune (cioè interne) sia quelle di diritto penale internazionale di origine convenzionale appaiono ispirate ai medesimi criteri, che la dottrina, con riguardo a fattispecie più tradizionali, cioè non relative a dati informatici, ha raggruppato in sei distinti principi idonei a fungere da titoli di *jurisdiction* in materia penale.

Cerchiamo di applicarli, operando i necessari adattamenti, all'oggetto della nostra indagine, per individuarne punti di forza e criticità.

a) Secondo un primo approccio, basato sul principio di territorialità[17], la competenza ad adottare provvedimenti siffatti apparterrebbe all'autorità giurisdizionale dello Stato sul cui territorio il *cloud* è collocato. Tuttavia, quello territoriale rappresenta, come evidente, un titolo legittimante che, qualora dovesse essere concepito come esclusivo,

14. Cfr. Quadri, *Diritto penale internazionale*, Padova, 1944, p. 34.

15. Per tutti v. Caracciolo, *Dal diritto penale,* cit., *passim*.

16. Cfr. Caracciolo, *Dal diritto penale*, cit., p. 33.

17. Sul principio in parola si veda la nota sentenza della Corte permanente di giustizia internazionale relativa al caso *Lotus* (Francia v. Turchia), che afferma che « *in all systems of law the principle of the territorial character of criminal law is fundamental* », sebbene poi chiarisca anche che il medesimo principio « *is not an absolute principle of international law and by no means coincides with territorial sovereignity* ». Il testo integrale della decisione è reperibile all'indirizzo *www.worldcourts.com*.

in assenza di accordi internazionali di cooperazione giudiziaria o, comunque, del consenso del sovrano territoriale[18], renderebbe illegittima l'acquisizione dei dati da parte di autorità estere rispetto al luogo di allocazione, con evidenti limitazioni all'attività investigativa e repressiva.

b) Una differente ricostruzione attribuisce invece, sulla base del principio di nazionalità, la legittimazione all'acquisizione in parola all'autorità del Paese di cui è cittadino il soggetto nei cui confronti si stanno svolgendo le indagini (c.d. principio della nazionalità attiva)[19]. Anche questa soluzione ci sembra sollevare, nel caso del *cloud computing*, più problemi di quanti non ne risolva, dal momento che consentirebbe all'autorità procedente, in assenza di cooperazione da parte del sovrano territoriale del luogo ove è localizzato il *server*, di prendere conoscenza esclusivamente dei dati dei propri cittadini, con evidenti difficoltà materiali (si pensi al caso della condivisione dei medesimi dati tra più individui dotati di cittadinanze differenti) e limiti all'efficacia delle attività investigative e repressive, specie se si considera la frequente transnazionalità dei gruppi criminali informatici.

c) Il medesimo criterio di collegamento viene utilizzato anche, nel caso del c.d. principio della nazionalità passiva, come titolo legittimante la giurisdizione dell'autorità nazionale del soggetto leso dal reato nei cui confronti si sta investigando o procedendo: anche questo approccio ci pare palesare limiti analoghi a quelli già sottolineati per la nazionalità attiva.

d) Il quarto criterio utilizzato come titolo legittimante l'esercizio della giurisdizione penale, stavolta con riguardo ai crimini commessi su navi e aeromobili, nonché sulle navi spaziali, è quello c.d. "della bandiera". Come noto, per il diritto internazionale i reati commessi su una nave o un aeromobile, in linea di massima (e cioè se non ledono gli interessi dello Stato titolare della sovranità della zona in cui il mezzo si trovava quando i fatti sono stati commessi), devono essere perseguiti dalla giurisdizione del Paese di cui la nave o l'aeromobile battono bandiera.

Si tratta di un principio che potrebbe essere interessante estendere al caso del *clouding*, in particolare per quei casi di eventuale allocazione dei *server*s al di fuori di zone sulle quali si esercita la sovranità esclusiva di uno Stato, come nelle ipotesi delle *server farms* oceaniche di Google alle quali abbiamo fatto riferimento nel par. 1. Tuttavia, anche in questo caso, come già sottolineato per il principio di territo-

18. Sul consenso del titolare dei dati come titolo legittimante l'acquisizione e, in particolare, l'art. 32, lett. *b)* della Convenzione del Consiglio d'Europa sulla criminalità informatica v. invece *infra* il par. succ.

19. Cassese, *International Criminal Law*, Oxford, 2003, p. 281 ss.

rialità, il titolo in parola legittimerebbe, se applicato *sic et simpliticer*, l'*enforcement* sui dati esclusivamente da parte dello Stato di bandiera. Il problema segnalato potrebbe essere risolto mediante criteri analoghi a quelli contenuti in alcune norme della Convenzione delle Nazioni Unite sul diritto del mare (CNUDM)[20], e in particolare nell'art. 109, relativo alle "Trasmissioni non autorizzate dall'altro mare". Il par. 3 di quest'ultimo prevede infatti che chiunque sia responsabile di trasmissioni non autorizzate che partano dal mare internazionale può essere sottoposto a procedimento giurisdizionale penale interno, oltre che dello Stato di bandiera della nave, anche dello Stato presso cui la stazione trasmittente è registrata, dello Stato nazionale di uno dei responsabili della trasmissione, di uno qualunque degli Stati che ricevono la trasmissione stessa o ancora di uno qualunque degli Stati le cui radiocomunicazioni autorizzate subiscono interferenze a cagione della stessa. In buona sostanza la CNUDM legittima, in materia di trasmissioni "pirata" dal mare internazionale, l'intervento autoritativo di qualsivoglia Stato i cui interessi siano stati così lesi. E agli stessi Stati, ai sensi del successivo par. 4 del medesimo art. 109, è riconosciuta la facoltà di procedere ad arrestare qualunque persona o fermare qualsiasi nave sia implicata nelle trasmissioni non autorizzate, nonché procedere al sequestro delle apparecchiature trasmittenti[21].

e) Un'applicazione più generale della *ratio* che abbiamo appena visto applicata nell'art. 109 della CNUDM, potrebbe poi comportare la legittimazione ad adottare misure di *enforcement* sui dati conservati su un *server* all'estero da parte di qualunque Paese i cui interessi siano stati lesi dal comportamento nei cui confronti si intende procedere. Si tratta, peraltro, di un approccio che non ci pare del tutto estraneo alla prassi, in particolar modo italiana, se si pensa che la giurisprudenza relativa alla diffamazione avvenuta a mezzo Internet per tramite di *server* localizzato all'estero, ritenendo che il reato di diffamazione, dotato di natura di reato di evento, si consumi « *nel momento e nel luogo in cui i terzi percepiscono l'espressione ingiuriosa*[22] », ha concluso per la sussistenza della giurisdizione italiana in tutti i casi di informazioni ospitate su *server* all'estero, nel momento in cui il messaggio

20. La Convenzione, che attualmente risulta ratificata da 156 Stati e dall'Unione europea, è stata aperta alla firma il 10 dicembre 1982 a Montego Bay, in Giamaica, dopo oltre 14 anni di negoziato. È entrata in vigore il 16 novembre 1994; il Parlamento italiano ha autorizzato la ratifica con la legge 2 dicembre 1994, n. 689.

21. In merito alla possibilità di applicazione ad Internet di norme di diritto internazionale ad essa preesistenti ci permettiamo di rinviare a Ruotolo, *Internet–ional Law*, *Profili di diritto internazionale pubblico della Rete*, Bari, 2012, p. 56. Con specifico riferimento all'argomento trattato nel testo, poi, cfr. Swanson, *Google Sets Sail: Ocean–Based Server Farms and International Law,* in *Connecticut Law Review,* 2011, 709 ss.

22. Cass., Sez. V, 27 aprile 2012, P.C. in proc Ayroldi, in *Mass. Uff.*, n. 252964

diffamatorio fosse venuto a conoscenza di persone che si trovano in Italia[23].

f) Ricordiamo infine come si vada progressivamente consolidando, con riguardo ai crimini internazionali degli individui, il principio di universalità della giurisdizione penale[24], il quale però, in considerazione dei reati cui è applicabile, difficilmente commissibili via *cloud*, ci pare sia di rilevanza marginale rispetto all'oggetto della nostra indagine.

4. Le pertinenti disposizioni della Convenzione del Consiglio d'Europa sulla criminalità informatica. Di alcuni dei criteri appena riassunti è fatta applicazione esplicita nel diritto internazionale pattizio, e segnatamente nella Convenzione del Consiglio d'Europa sulla criminalità informatica[25].

Ricordiamo che la Convenzione, dopo una serie di norme definitorie di importanza centrale per la ricostruzione del regime di diritto internazionale di *governance* di Internet[26], impone agli Stati membri l'inserimento, nei propri ordinamenti nazionali, di specifiche norme di diritto penale sostanziale (Capitolo II, sezione I: art. da 2 a 13) — tra le quali i reati di accesso senza legittimazione ai sistemi informatici, di attentato all'integrità di dati e sistemi, di falsificazione e frode, nonché i reati collegati alla pornografia minorile e alla violazione di diritti di proprietà intellettuale — e norme di natura processuale relative al perseguimento dei reati così introdotti (Capitolo II, sezione II: artt. da 14 a 22), e al rafforzamento degli strumenti di cooperazione internazionale in materia (Capitolo III: art. da 23 a 35). Chiudono il testo della Convenzione le disposizioni finali relative a firma, ratifica, entrata in vigore, modalità di adesione, ambito territoriale di applicazione e strumenti di soluzione delle controversie sull'applicazione e l'interpretazione della Convezione medesima (Capitolo IV: artt. da 36 a 48).

Ebbene, con esplicito riguardo all'apprensione d'autorità di dati su *server* la Convenzione, all'art. 19 ("Perquisizione e sequestro dati di informatici immagazzinati") impone a ogni Stato membro di adottare le misure necessarie per consentire alle proprie autorità nazionali di perquisire o accedere a un sistema informatico e ai dati che esso contiene, nonché ai supporti per la conservazione di dati informatici nel quale i dati stessi possono essere immagazzinati, nel proprio territorio: la disposizione in commento, tuttavia, ha

23. Secondo Cass., Sez. II, 21 febbraio 2008, Buraschi e altro, in *Mass. Uff.*, n. 242085, infatti, « *il reato di diffamazione consistente nell'immissione nella rete Internet di frasi offensive e, o immagini denigratorie, deve ritenersi commesso nel luogo in cui le offese e le denigrazioni sono percepite da più fruitori della rete, pur quando il sito "web" sia registrato all'estero* ».

24. V. Zappalà, *L'universalità della giurisdizione sui crimini internazionali: "dittatura dei virtuosi" o tutela diffusa dei valori universali?* in *Ordine internazionale e valori etici — Atti del VII Convegno della Società italiana di diritto internazionale*, a cura di Boschiero, Napoli, 2004, p. 308 ss.

25. La Convenzione, aperta alla firma il 21 novembre 2011, è entrata in vigore l'1 luglio 2004.

26. Cfr. Ruotolo, *Internet (diritto internazionale),* in *Enc. Dir. — Annali,* in corso di pubblicazione.

esclusivamente lo scopo di imporre ai Membri l'inserimento nei rispettivi ordinamenti nazionali, qualora i medesimi non le prevedano già, di norme volte a legittimare sequestri e perquisizioni di dati informatici che siano già all'interno della sfera della sovranità nazionale, senza nulla dire in merito all'eventualità che i dati o finanche tutto il sistema cui è necessario accedere siano all'estero.

Di quest'ultimo profilo si occupa quindi l'articolo 22, che impone agli Stati membri di adottare tutte le misure necessarie per stabilire la propria giurisdizione in merito ai reati previsti dalla Convenzione stessa (in particolare a quelli di cui agli dagli articoli da 2 a 11) quando i medesimi siano commessi:

a) nel proprio territorio;
b) a bordo di una nave battente bandiera di quella Parte contraente;
c) a bordo di un aeromobile immatricolato presso quella Parte;
d) da un proprio cittadino, a condizione che il fatto sia previsto come reato dalla legge del luogo dove è stato commesso o non rientri nella competenza territoriale di alcuno Stato[27].

L'art. 32 della stessa Convenzione completa il quadro descritto prevedendo il consenso del titolare come titolo legittimante l'acquisizione di dati: la disposizione in parola, rubricata « *Accesso transfrontaliero a dati informatici immagazzinati con il consenso o quando pubblicamente disponibili* », permette così a ogni Stato membro, senza avere riguardo al luogo geografico in cui sono archiviati e, quindi, senza che a tal fine sia necessario il consenso della Parte contraente sul cui territorio è allocato il *server* cui accedere, di acquisire tutti i dati disponibili al pubblico[28], nonché di accedere o ricevere nel proprio territorio dati immagazzinati in un altro Stato, previo « *consenso legale e volontario della persona legalmente autorizzata a divulgare i dati* ».

Le disposizioni appena esaminate sono volte ad accrescere la possibilità che le Autorità di un Paese membro possano legittimamente accedere ai dati contenuti in un *cloud server* di un altro Paese membro, ma non sono idonee a risolvere eventuali conflitti di giurisdizione, che pure potrebbero insorgere: l'assenza, nel sistema della Convenzione, della funzione di coordinare tra loro gli ordinamenti dei Paesi membri nel senso di regolare siffatti conflitti, peraltro, è confermata dal successivo par. 5 del già citato art. 22, il quale si limita ad auspicare che la Parte contraente che rivendichi la

27. Cfr. Sarzana di S. Ippolito, *Informatica, Internet e diritto penale*, Milano, 2012, p. 612 ss.

28. Al riguardo, per un esempio, si pensi ai dati inseriti su un *social network* senza che il titolare, nelle impostazioni della *privacy* del suo profilo, preveda alcuna limitazione in merito alla loro conoscibilità da parte di terzi. In merito a dati siffatti, in buona sostanza, è il loro titolare a fornire una volta per tutte il consenso alla loro diffusione pubblica e, quindi, alla loro apprensione da parte di chiunque, autorità comprese.

propria competenza penale in merito a una presunta infrazione prevista dalla Convenzione inviti a consultazione le altre Parti contraenti coinvolte "al fine di stabilire la competenza più appropriata per esercitare l'azione penale".

Al riguardo, quindi, la Convenzione non prevede neppure un obbligo *de negotiando,* limitandosi a invitare gli Stati i cui ordinamenti siano in potenziale o effettivo conflitto a una consultazione "laddove sia opportuno": anziché prevedere meccanismi automatici e, quindi, prevedibili di riparto della competenza all'azione penale e all'acquisizione dei dati, la Convenzione prevede solo un obbligo di cooperazione tra gli Stati membri, lasciando a un mero negoziato, peraltro neppure obbligatorio, il compito di dirimere il nodo che si dovesse eventualmente essere creato.

5. Il *power of disposal* come titolo di giurisdizione e la Bozza di Protocollo addizionale alla Convenzione sulla criminalità informatica. Molti dei limiti che abbiamo visto caratterizzare i criteri sin qui enunciati potrebbero però essere superati se si riuscisse a individuare un fattore di collegamento relativo direttamente ai dati e non già ai loro titolari (come la cittadinanza) o alla localizzazione del *server* che li ospita, elementi, questi ultimi, che potrebbero essere sconosciuti o comunque non facilmente conoscibili.

Proprio al fine di superare i limiti connessi alla "delocalizzazione" delle fattispecie di *cloud computing*, uno studio della Divisione su crimine economico della Direzione generale del Consiglio d'Europa[29], muovendo dal presupposto che « *neither the existing solution of access with consent nor general principles of international law measure up to the specific challenge created by the loss of location* »[30], ha ipotizzato l'utilizzazione del c.d. *power of disposal* ("potere dispositivo"), come criterio di collegamento nella materia che ci occupa. La persona titolare di tale potere sarebbe, secondo questa ricostruzione, chi detiene il diritto di modificare, cancellare, sopprimere o rendere inutilizzabili i dati o, ancora, di escludere chiunque altro da ogni accesso ai medesimi. Ora, come è noto, la prassi vuole che la legittimazione all'accesso a un sistema informatico sia generalmente attestata dal possesso di credenziali di autenticazione (nome utente e *password*, quanto meno): secondo la proposta in esame, quindi, una data autorità nazionale potrebbe essere legittimata ad accedere a tutti i dati, ovunque detenuti e indipendentemente dalla nazionalità del loro titolare, conservati su un *cloud* di cui sia riuscita ad ottenere, in modo legale (ad esempio mediante un'intercettazione regolarmente au-

29. *Discussion paper on Cloud Computing and cybercrime investigations*: *Territoriality vs. the power of disposal*?, 10 agosto 2010, *ww.coe.int*.

30. Cfr. il par. 3.2 dello studio cit. alla nota precedente. In generale sulla progressiva perdita di rilevanza del concetto di territorialità nelle norme di diritto internazionale che riguardano Internet ci permettiamo di rinviare a Ruotolo, *The Impact of the Internet on International Law:* nomos *without Earth*?, in *Informatica e diritto*, 2013, 2, 7 ss.

torizzata), le credenziali di accesso, senza che a tal fine sia stata chiesta la collaborazione del loro titolare o del fornitore del servizio di *cloud*.

Un approccio siffatto, del tutto sganciato da ogni riferimento territoriale e personale, consentirebbe alle autorità procedenti di operare senza che sia necessario conoscere preventivamente il contenuto dei dati o il luogo di localizzazione del *cloud*, e, quindi, di superare molti dei limiti palesati da criteri di legittimazione più tradizionali ma, nel contempo, potrebbe comportare una violazione anche grave dei diritti fondamentali della persona sottoposta alle indagini o finanche di soggetti terzi. Potrebbe quindi essere opportuno delimitare l'ambito di applicazione del criteri in parola ai soli casi in cui vi sia il documentato rischio di distruzione dei dati da parte del sospettato, e sotto il profilo procedurale, prevedere l'autorizzazione dell'autorità giudiziaria, l'obbligo della notifica, sia al titolare del *power of disposal* sia al fornitore del servizio di *cloud*, dell'avvenuto accesso ai dati e una qualche forma di *judicial review*. Su queste premesse il Comitato della Convenzione sulla criminalità informatica (*Cybercrime Convention Committee*), nell'aprile 2013, ha pubblicato i « *(Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding transborder access to data* »[31], al fine di proporre una soluzione di diritto positivo a questi temi sotto forma di un protocollo alla Convenzione di Budapest. Il *Draft* in questione contiene ben cinque distinte proposte d'integrazione dell'art. 32 della Convenzione del quale abbiamo detto *supra*: se alcune di queste appaiono ragionevoli, come quelle che intendono recepire nel sistema della Convenzione il criterio del *power of disposal* di cui abbiamo appena detto[32], e consentire l'accesso ai dati in assenza del consenso del loro titolare, ma mediante "lawfully obtained credentials", piuttosto singolare appare la proposta che, nell'intento di fissare un titolo di legittimazione universalmente applicabile, suggerisce di estendere le norme della Convenzione che legittimano l'acquisizione dei dati su *cloud* all'estero finanche ai *servers* ospitati sul territorio di Stati che non siano parte della Convenzione stessa. Non si comprende in assenza sia di norme di diritto internazionale generale sia di una qualche prassi significativa, quale possa essere il titolo legittimante una siffatta "universalizzazione" di una norma di diritto internazionale pattizio, dal momento che, come noto, l'art. 34 della Convenzione di Vienna sul diritto dei trattati del 23 maggio 1969 prevede che un trattato non possa creare né obblighi né diritti per uno Stato terzo senza il consenso di quest'ultimo[33].

Da ultimo, il 5 novembre 2013, il gruppo di studio « *on Transborder Access and Jurisdiction* » del Consiglio d'europa ha pubblicato il suo rapporto per il

31. Doc. T–CY (2013)14, del 9 aprile 2014, reperibile all'indirizzo *www.coe.int*.

32. Si tratta della proposta n. 5, « *The power of disposal as connecting legal factor* ».

33. Peraltro gli stessi redattori del *draft* riconoscono che « *this option may raise concerns of international law. Article 34 of the Vienna Convention on the Law of Treaties does not allow a treaty to create obligations or rights for a third State without its consent* ».

2013[34] in cui ribadisce la necessità di un bilanciamento tra l'interesse pubblico ad indagini penali rapide ed efficaci ai fini di contrasto alla criminalità e i diritti individuali, e che, di conseguenza, tutte le soluzioni eventualmente adottate in merito all'accesso transfrontaliero ai dati dovranno essere accompagnate da garanzie e condizioni per tutelare i diritti degli individui e prevenire l'uso improprio dei meccanismi così disciplinati.

Il medesimo rapporto, peraltro, consolidando quel paradigma *multistakeholder* che, a nostro giudizio, caratterizza tutti i procedimenti posti in essere nell'ordinamento internazionale al fine di adottare norme di disciplina di fattispecie che si realizzano *on–line*[35], sottolinea la necessità di un dialogo con le autorità per la protezione dei dati, la società civile e le organizzazioni del settore privato, e rinvia ogni decisione all'esito di un'ulteriore riflessione, da concludersi entro il 31 dicembre 2013.

34. *Report of the Transborder Group for 2013*, T–CY (2013)30, in *www.coe.int*.

35. Cfr. Ruotolo, *Internet–ional Law*, cit., p. 144 ss.