Vincenzo Zeno-Zencovich

Intorno alla decisione nel caso Schrems*: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*

SOMMARIO: 1. La crescente problematica della 'sovranità digitale'. – 2. Sovranità come giurisdizione. – 3. La sovranità sui segmenti materiali di una rete. – 4. Il 'territorio' di Internet. – 5. I precedenti del mare, del cielo, dello spazio. – 6. Le sedi internazionali per il governo delle reti digitali. – 7. Una visione d'insieme sulla 'sovranità digitale'.

1. La crescente problematica della 'sovranità digitale'

La decisione della Corte di Giustizia UE nel caso *Schrems* costituisce un passo ulteriore per l'affermazione di una 'sovranità digitale' dell'Unione Europea. Il termine 'sovranità' è qui utilizzato nel suo senso tradizionale: il potere di controllare, *de iure e de facto*, un certo spazio, le attività che ivi si svolgono, coloro che vi entrano, come tale spazio è organizzato, amministrare poteri di polizia, giudiziari e di sicurezza in tale spazio.

Quando la Corte di Giustizia nella sua decisione del 2014 nel caso *Google Spain*[1] ha affermato che (dilatando notevolmente il concetto di 'stabilimento' e swuscitando non poche perplessità sulla coerenza della decisione sui numerossisimi precedenti della Corte) Google deve considerarsi stabilita nell'Unione Europea ed è quindi soggetta al diritto UE, essa sta affermando la sovranità su entità economiche che operano all'interno dello spazio europeo, sia pure attraverso reti di telecomunicazione che consentono l'uso di Internet.

Quando la stessa Corte, un anno più tardi, afferma che il trasferimento

[1] *Google Spain v. Agencia Española de Protecciòn de Datos, Costeja*, C-131/12, of May 13, 2014. La decisione ha raccolto decine di commenti. Per una rassegna esaustiva della varie tematiche si veda il Volume speciale n. 4-5 /2014 di *Dir. Inf.*. I vari contributi sono raccolti ora in G. Resta – V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza* Google Spain, Roma TrE-Press, 2015 [disponibile on-line alla pagina http://ojs.romatrepress.uniroma3.it/index.php/oblio].

di dati personali di cittadini europei verso Stati Uniti non è lecito, essa sta affermando, in sostanza, che il trattamento dei dati personali è regolato dal diritto UE, non dal diritto di un altro Stato.

La circostanza che entrambi i casi riguardano dati personali[2] non deve trarre in inganno. Il trattamento dei dati personali è considerato uno dei tratti distintivi del sistema giuridico europeo, uno dei suoi valori pre-giuridici, contrapposti ad un approccio statunitense significativamente diverso allo stesso tema. Tuttavia ciò ha solo reso più facile – grazie anche a quel che appare una attenta selezione della priorità dei casi da esaminare[3] – per la Corte di Giustizia adottare decisioni dirompenti che sconfessano accordi di alto livello delle istituzioni comunitarie. Fino alla decisione nel caso *Google Spain* vi era la diffusa convinzione che il trattamento dei dati da parte del grande motore di ricerca, che è presente in praticamente ogni momento della nostra vita, doveva ritenersi effettuato sui 'mainframe' presenti negli Stati Uniti, e quindi non fosse soggetto alla direttiva UE sui dati personali. E il trasferimento di dati verso quel Paese era coperto dall'accordo internazionale «Safe Harbour» il quale, asseritamente, doveva garantire un analogo livello di protezione nel trattamento dei dati al di là dell'Atlantico.

In quest'ultimo caso il profilo della sovranità è molto più evidente, in quanto il *casus belli* è esplicitamente individuato nell'esercizio di poteri sovrani da parte degli Stati Uniti sui dati europei sulla base dell'irresistibile «Patriot Act».

La Corte di Giustizia dunque, a guardare le cose in una prospettiva realista, sta affermando che il Consiglio UE ha inammissibilmente rinunciato all'esercizio dei suoi poteri sovrani nello stipulare l'accordo «Safe Harbour» con gli Stati Uniti. La Corte – utilizzando la materia particolarmente sensibile dei diritti fondamentali – sta segnando il confine dei

[2] Cosa intendiamo per 'dati'? Sulla distinzione fra dati dinamici, dati statici e metadata v. T. Maurer et al., *Technological Sovereignty: Missing the Point?*, in M. Maybaum, A-M. Osula, L. Lindstrom (a cura di), *7th International Conference on Cyber Conflict*, 2015 NATO CCD COE Publications, (a p. 56) disponibile on-line alla pagina https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2004%20Technological%20Sovereignity%20-%20Missing%20the%20Point.pdf [ultimo accesso 10.7.2016].

[3] Pochi giorni prima della sentenza *Schrems*, la CGUE ha emesso due sentenze nei casi *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság* (C-230/14) e *Smaranda Bara and Others c. Preşedintele Casei Naţionale de Asigurări de Sănătate and Others* (C-201/14). Nel primo caso si trattava della applicabilità dei diritto ungherese al trattamento dei dati personali da parte di un fornitore di servizi stabilito in Slovacchia (Il diritto UE sui dati personali è «nel senso che esso consente l'applicazione della legge in materia di protezione dei dati personali di uno Stato membro diverso da quello nel quale il responsabile del trattamento di tali dati è registrato»). Nel secondo caso ha statuito che il trasferimento, senza previo consenso, di dati fiscali personali ad un istituto di previdenza sociale non è consentito in base al diritto UE.

poteri sovrani e, molto chiaramente, statuendo la supremazia giudiziale su temi del più alto livello politico, come la politica internazionale. La sentenza *Schrems* richiede pertanto di essere analizzata nella prospettiva di due super-potenze internazionali che si fronteggiano per il controllo di una risorsa essenziale quale le reti globali di telecomunicazioni. Questo confronto era già emerso con riferimento ai casi SWIFT (dati delle operazioni bancarie)[4] e PNR (dati dei passeggeri del trasporto aereo)[5] nei quali, inconsapevolmente o coattivamente, i dati venivano trasmessi negli Stati Uniti e utilizzati dalle sue autorità. In questo caso si è passati ad un livello più ampio e generale perché comprende ogni sorta di dati, dalle fonti più diverse, consentendo una profilazione più accurata.

2. Sovranità come giurisdizione

Anche se questa non è la sede per una approfondita analisi della casistica giurisprudenziale e istituzionale, vale la pena osservare che non vi è alcuna ragione per la quale le reti di telecomunicazioni e tutte le attività che vi si svolgono direttamente o indirettamente non debbano formare oggetto di grande attenzione da parte delle super-potenze, considerando la loro importanza in tutti i campi. In questo contesto più generale si è tuttavia portati a considerare alcuni aspetti specifici non solo perché il punto di partenza è una decisione della più alta Corte dell'Unione Europea, ma anche perché essa deve essere confrontata con le decisioni di altre corti al di là dell'Atlantico[6]. Qui il concetto di sovranità si traduce nel termine elegante e tecnico di giurisdizione. Ma è del tutto evidente che stabilire che una Corte è competente a conoscere una certa controversia – e dunque ha giurisdizione – costituisce l'espressione di poteri sovrani, e solitamente questa decisione viene assunta direttamente dalle corti stesse. D'altronde

[4] Si v. l'accordo «tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi» in GUUE L8 del 13.1.2010.

[5] Si v. l'«Accordo tra gli USA e l'UE sull'uso e sul trasferimento del codice di prenotazione (Passenger Name Record — PNR) al Dipartimento per la sicurezza interna degli Stati Uniti» in GUUE L215 dell'11.8.2012.

[6] Si v. ad es *In re Microsoft*, 15 F. Supp. 3rd 466 (S.D.N.Y 2014) ove si è stabilito che i dati detenuti da Microsoft in Irlanda cadessero sotto la giurisdizione statunitense e dunque assoggettabili ad un mandato di acquisizione emesso sulla base dell'Electronic Communications Privacy Act, come modificato dal Patriot Act.

il potere di fissare norme si associa a quello di stabilire come, quando e in che misura tali norme possono o devono essere applicate. In questa prospettiva, anche se, per ipotesi, la Corte di Giustizia avesse statuito che l'accordo di «Safe Harbour» era perfettamente conforme al diritto comunitario, la decisione sarebbe stata comunque l'espressione di un potere sovrano. Bisogna poi aggiungere – e la notazione vale ancor più nel caso di reti di comunicazione elettronica – che non è sufficiente affermare la sovranità giacchè questa deve essere riconosciuta (o, almeno, subita) anche da altri Stati, senza contare le diverse situazioni di possibile interferenza fra giurisdizioni di cui venga negata la esclusività, ponendo questioni in ordine alla concorrenza fra di esse ed i criteri per evitare il rischio di conflitto fra decisioni. La sentenza Schrems è utile, da questo punto di vista, perché serve a scartare una certa idea delle attività sulle reti di telecomunicazione, e sul più noto protocollo di comunicazione, Internet, come se fosse a-territoriale e quindi non soggette a sovranità statale[7]. Questa idea – che risale alla prima epoca di Internet e al suo sviluppo spontaneo[8] – è stata ampiamente superata dalla progressiva espansione dell'intervento statale e dalla regolazione delle reti e delle attività che su di esse vengono condotte.

3. La sovranità sui segmenti materiali di una rete

Le reti di telecomunicazioni sono composte in larga parte da elementi fisici (cavi, centraline, elaboratori, trasmettitori) che devono essere posizionati da qualche parte all'interno del territorio dello stato. Anche quando la rete utilizza significativi segmenti di comunicazioni *wireless*, queste devono essere trasmesse e ricevute da antenne e radio-basi. Su queste componenti lo Stato esercita legittimamente i propri poteri o imponendo che operino sulla base di talune regole tecniche ed amministrative[9]. La

[7] L'idea è contestata da W. Heintschel Von Heinegg, *Legal Implications of Territorial Sovereignty in Cyberspace*, in C. Czosseck, R. Ottis, K. Ziolkowsky (a cura di), *4th International Conference on Cyber Conflict*, 2012 NATO CCD COE Publications, p.9 (disponibile on-line alla pagina https://ccdcoe.org/sites/default/files/multimedia/pdf/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf [ultimo accesso 10.7.2016]).

[8] Tuttavia era già stata messa in discussione quasi vent'anni fa: v. T.S. WU, *Cyberspace Sovereignty? The Internet and the International System*, 10 *Harv. J. L.&Tech*. 647 (1997).

[9] In questo senso v. W. Heintschel Von Heinegg, *Legal Implications etc*.,cit. alla nt. 7, p.9 s. «La circostanza che le componenti dell'Internet si trovino nel territorio sovrano dello Stato ma formano, allo stesso tempo, parte dell'Internet globale, non indica che

circostanza che le trasmissioni siano intangibili non significa che lo Stato non possa, *de facto* e *de iure*, impedire la circolazione di taluni contenuti, l'accesso a siti stranieri, o l'accesso dall'esterno a siti interni, e in generale non possa legittimamente – come normalmente e regolarmente fanno anche i paesi democratici – controllare e acquisire il contenuti di comunicazioni digitali. Tutti questi interventi costituiscono segno evidente che gli stati – o nel caso dell'UE, entità sopra-nazionali alle quali gli Stati hanno conferito taluni poteri – esercitano i loro poteri sovrani sulle reti di telecomunicazioni, da aspetti minuti fino a interventi assai più complessi e profondi. Stabilire come i dati personali raccolti attraverso le reti di telecomunicazioni debbano e/o possono essere elaborati e a quali condizioni essi possano essere trasferiti in altri paesi costituisce semplicemente l'espressione dell'esercizio di poteri sovrani da parte e secondo uno stato di diritto. Il diritto, sotto forma di un provvedimento generale ovvero di una decisione giudiziale, stabilisce quel che legittimamente può essere fatto. Per le parti che non vi si conformano vi saranno sanzioni di progressiva incisività fino alla chiusura di talune attività e l'arresto delle persone fisiche che le svolgono.

Sarebbe ingenuo ritenere che questa manifestazione di poteri sovrani sia una particolarità del modello giuridico e politico europeo[10]. Negli Stati Uniti il governo delle reti globali è stato ed è attribuito in maniera significativa ad attori privati i quali operano all'interno del sistema giuridico statunitense. Il primo e ovvio esempio è quello di ICANN, l'organismo cui è attribuito il compito di fissare i criteri per l'attribuzione dei nomi di domino e altre procedure per l'attività attraverso Internet[11]. Ma anche quando grandi prestatori di servizi sulla rete (come Google, Facebook, E-bay, Wikipedia, ecc.), nelle loro condizioni generali di servizio statuiscono che il diritto applicabile è il diritto statunitense, spesso indicando un foro domestico, essi stanno in sostanza affermando che il diritto americano, e quindi i poteri sovrani degli Stati Uniti, governano la rete globale.

vi sia stata una rinuncia all'esercizio della giurisdizione territoriale» (così K. Ziolkowsi, *General Principles of International Law as Applicable in Cyberspace*, in K. Ziolkowsi (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, 135, at p.162) disponibile on-line alla pagina https://ccdcoe.org/publications/books/Peacetime-Regime.pdf [ultimo accesso 10.7.2016].

[10] La preoccupazione per un crescente *Data Nationalism* è espressa da A.Chander, U.P.LE, 64 *Emory L.J* 677 (2015).

[11] L'ICANN si qualifica come una ONG ma è retta dal diritto statunitense e agisce per conto dello US Department of Commerce, al quale fa riferimento: see K. Ziolkowsi, *General Principles of International Law as Applicable in Cyberspace*, cit. alla nt. 9, p. 157.

Questo conflitto – in primo luogo un conflitto di sistemi e dunque un conflitto di ordinamenti giuridici – non appare risolubile attraverso le ben note e sperimentate regole del diritto internazionale privato e processuale[12]. Il problema, infatti, non è quello di stabilire quale diritto privato debba applicarsi al rapporto giuridico e chi sia il giudice competente. Quel che è in gioco in questi casi, invece, è la regolazione pubblica delle reti, che non può essere risolto attraverso le regole applicabili ai soggetti privati.

Utilizzando il caso deciso dalla Corte di Giustizia, la decisione non riguarda i dati personali del sig. Schrems (in ipotesi, Facebook avrebbe potuto impegnarsi ad accantonare i suoi dati e trattarli in Europa), ma piuttosto i dati personali di tutti i cittadini europei. Si tratta di una questione che non può essere affrontata e risolta attraverso gli strumenti e un contenzioso di diritti privato.

4. Il 'territorio' di Internet

Come s'è detto, la circostanza che i dati personali siano stati presi nel caso *Schrems* come oggetto di contesa con gli Stati Uniti non significa in alcun modo che i suoi effetti siano limitati a questo profilo[13]. Si può agevolmente immaginare l'estensione del diritto comunitario, e dunque della sovranità dell'UE, a operazioni di commercio fra l'Europa e gli Stati Uniti; all'applicazione del diritto europeo della proprietà intellettuale o della concorrenza a «big-data» conservati al di là dell'Atlantico ma comprendenti un numero significativo di dati 'europei'; o la possibilità e i limiti del trattamento di dati pubblici al di fuori dei confini dell'Unione[14]; fino al controverso tema della

[12] Le quali in ogni caso sono rese ancor più complesse dalla ubiquità dell'Internet v. D.J.B. Svantesson, *Sovereignty in International Law - How the Internet (Maybe) Changed Everything, But Not for Long,* in 8 *Masaryk U. J.L. & Tech*. 137 (2014). Il ragionamento è sviluppato dallo stesso A. in *A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft*, 2015 *Am.J.Int'l L.Unbound*, disponibile on-line alla pagina https://www.asil.org/blogs/new-jurisprudential-framework-jurisdiction-beyond-harvard-draft [ultimo accesso 10.7.2016].

[13] V. T. Maurer et al., *Technological Sovereignty*, cit. alla nt. 2.

[14] L'approccio prospettato da J. Daskal, *The Un-Territoriality of Data*, in *Yale L.J* (2016) è che i dati non sono connessi ad alcuno specifico territorio; e sono slegati dalla cittadinanza. Almeno nell'UE questa seconda affermazione non sembra condivisibile. La protezione dei dati personali è riconosciuta come diritto fondamentale dall'art.8 della Carta Europea dei Diritti Fondamentali e dunque si tratta di una situazione giuridica strettamente legata alla cittadinanza europea. Per le complesse questioni anche di ordine

tassazione delle attività in rete. Una delle ovvie conseguenze della decisione della Corte di Giustizia è la necessità di definire chiaramente i confini della sovranità dell'UE sulle reti di telecomunicazione.

In primo luogo, dove cominciano e dove finiscono?[15] La risposta non è ovvia considerando il gran numero di stati europei che hanno estensioni oltremare: si pensi alla Danimarca con la Groenlandia, i Paesi Bassi con i possedimenti nelle Antille, la Francia con i suoi DOM e TOM, e il Regno Unito con le dozzine di isole disseminate in ogni oceano del mondo. Si deve poi considerare che gran parte degli abitanti di tali luoghi assai distanti hanno una cittadinanza europea e dunque vantano gli stessi diritti dei cittadini della madre-patria e sono soggetti alle stesse leggi. E i cittadini – e la cittadinanza – sono uno degli elementi essenziali della sovranità[16].

Questo elemento richiede di essere attentamente considerato in una molteplicità di casi:

a. Quando un cittadino dell'Unione accede la rete dall'Europa e raggiunge un sito extra-UE

b. Quando un cittadino extra-comunitario accede, da fuori dell'Europa, un sito che ha sede in Europa.

c. Quando un cittadino europeo, che si trova al di fuori dell'Unione, accede un sito che si trova all'interno[17].

---

costituzionale che risultano dall'uso del 'cloud computing' nel campo dei dati detenuti da soggetti pubblici (e quindi oggetto di un potere sovrano di controllo e comando) e la interazione con il diritto UE v. F. Cardarelli, *Amministrazione digitale, trasparenza e principio di legalità*, in *Dir. Inf.* 2015, 227 (p. 250 s.).

[15] V. P.W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 *Air Force L.Rev*. 1 (2009): «Gli stati devono essere in grado di stabilire una frontiera nel ciber-spazio che uno stato può sia sorvegliare che controllare. Se non si è in grado di svolgere tale funzione, il concetto di sovranità nel ciber-spazio è priva di significato» (p. 39).

[16] Si sostiene che nei casi in cui i dati sono trattati (asseritamente in maniera illegittima) al di fuori dell'Unione, la UE applicherebbe il principio della c.d. personalità passiva (v. B. Pirker, *Territorial Sovereignty and Integrity and the Challenges of Cyberspace*, in K. Ziolkowsi (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, 189 (a p. 196) disponibile on-line alla pagina https://ccdcoe.org/publications/books/Peacetime-Regime.pdf [ultimo accesso 10.7.2016]. Per un approccio che collega giurisdizione a cittadinanza v C.RYNGAERT, M. Zoetekouw, *The End of Territory? The Re-Emergence of Community as a Principle of Jurisdictional Order in the Internet Era*, disponibile on-line alla pagina http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2523354 [ultimo accesso 10.7.2016].

[17] Questo approccio è diverso da quello seguito da W. Heintschel Von Heinegg, *Legal Implications etc*., cit. alla nt.7 (p. 15) nel caso della giurisdizione nei confronti di taluno

È chiaro che la crescente tensione fra il bisogno di una rete aperta e autenticamente globale e l'affermazione di diritti di sovranità sul proprio territorio e sui propri cittadini richiede, per risolverla, più della semplice buona volontà[18].

Il primo punto da considerare è quel che si potrebbe definire l'atteggiamento mentale. L'idea dominante, per lungo tempo, è stata – come si è visto in apertura – che l'Internet, in quanto globale, è essenzialmente a-territoriale e può vivere grazie a regole auto-determinate. Dietro queste idea sembrano esserci diversi fraintendimenti.

a. Per dire le cose con una certa crudezza, nella prospettiva della sovranità, Internet non esiste. Esso è soltanto un protocollo per trasferire messaggi (pacchetti di dati) utilizzando reti pubbliche (*id est* aperte al pubblico) di telecomunicazioni. È chiaro che questo protocollo ha consistenza giuridica nel mondo della proprietà intellettuale e dal punto di vista regolamentare, ma essendo interamente non materiale esso non può formare oggetto di sovranità più di uno standard di telecomunicazione o di un sistema di misurazione metrico decimale. Non vi è sovranità sul protocollo Internet più di quanta ce ne possa essere sui protocolli utilizzati per i servizi Skype o WhatsApp.

b. Questo protocollo oggi esiste ed è utilizzato, ma nel futuro potrebbe essere sostituito da altre tecnologie o, molto semplicemente, alcuni Stati potrebbero decidere di usare standard delle comunicazioni su rete non compatibili con il protocollo Internet[19].

c. Il fatto che gli impulsi digitali che vengono trasmessi sono intangibili e vengono inviati grazie ad una entità non materiale (come il protocollo Internet) non significa in nessun modo che la rete sia immateriale. Essa, invece, è composta in larga misura da elementi fisici, collocati quasi interamente sul territorio sovrano dello Stato. L'unico caso di comunicazione extra-territoriale non-materiale è quella

il quale, dall'estero, abbia commesso atti dannosi «contro la infrastruttura digitale di un altro Stato». Il caso proposto nel testo, invece, è se coloro i quali operano attraverso Internet possono godere della protezione della legge di uno Stato, e se entità poste al di fuori del suo territorio possano essere tenuti al rispetto delle norme di un diverso Stato.

[18] Il rischio paventato è quello di una «Balcanizzazione dell'Internet in una molteplicità di sistemi chiusi protetti dall'accesso extra-territoriale di ISP situati all'estero» (J. Daskal, *The Un-Territoriality of Data*, cit. alla nt. 14, a p. 332). Simili preoccupazioni sono espresse A. Chander, U.P.LE, *Data Nationalism*, cit. alla nt. 10.

[19] Si tratta di una situazione comune nel passato: basti pensare alla vicenda, risalente agli anni '70 e '80 del secolo scorso con riguardo agli standards (fra loro incompatibili) per la televisione a colori (PAL, tedesco; e SECAM, francese).

di un messaggio proveniente da un satellite ricevibile direttamente dall'utente (ad es. con un telefono mobile satellitare) senza bisogno di una infrastruttura terrestre che lo distribuisca[20].

d. Gli Stati controllano i segmenti fisici delle rete di comunicazione e decidono quali standards vogliono accettare. Quindi sono gli Stati a decidere se vogliono ammettere, ed entro quali limiti, Internet sulle proprie reti. Internet non ha territorio – e dunque non pone questioni di sovranità – perché da un punto di vista tecnico non ne può avere uno: non 'possiede' (nel senso di controllare e comandare) cavi, satelliti, frequenze. Queste sono controllate dagli Stati, o altre entità sopra-nazionali le quali regoleranno Internet ed ogni altra tecnica digitale utilizzata per comunicare attraverso le reti, e tenderanno a farlo in maniera crescente[21].

5. I precedenti del mare, del cielo, dello spazio

Si dovrebbe, piuttosto, considerare che le reti di telecomunicazioni sono uno straordinario mezzo di comunicazione come lo è stato, fin dall'antichità, il mare e, dal XX secolo, lo sono il cielo e lo spazio[22].

[20] V. M. Mejia-Kaiser, *Space Law and Unauthorised Cyber Activities*, in K. Ziolkowsi (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, 349. Tuttavia – almeno con riguardo ad Internet – non si tratta della situazione ordinaria. L'equivoco ('L'errore fondamentale') è chiaramente evidenziato da I. Walden. *International Telecommunications Law, the Internet and the Regulation of Cyberspace,* in K. Ziolkowsi (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, 261 (a p. 266) disponibile on-line alla pagina https://ccdcoe.org/publications/books/Peacetime-Regime.pdf [ultimo accesso 10.7.2016].

[21] V. P.W. Franzese, *Sovereignty in Cyberspace*, cit. alla nt.15 : «Gli stati hanno la capacità di trasformare il ciber-spazio in un dominio sul quale possono esercitare la loro sovranità»(p.34).

[22] Già quasi 20 anni fa D.C. Menthe, in *Jurisdiction in Cyberspace: A Theory of International Spaces,* 4 *Mich. Telecomm. Tech. L. Rev.* 69 (1998) proponeva di qualificare il ciber-spazio come uno 'spazio internazionale' come l'Atartide, lo spazio extra-terrestre e l'alto mare. «Appare logico assimilarle all'alto mare, allo spazio aereo internazionale, allo spazio extra-terrestre»: W. Heintschel Von Heinegg, *Legal Implications etc.*, cit. alla nt. 7 , p.9; v. anche P.W. Franzese, *Sovereignty in Cyberspace*, cit. alla nt.15 (p. 40 s.). La similitudine è utilizzata anche per stabilire la giurisdizione in questioni di diritto internazionale privato: v. W.Guillermo Jimenez, A.R. Lodder, *Analyzing Approaches*

La circostanza che nessuno fisicamente possieda le onde del mare, l'aria attraverso la quale volano gli aerei o sono trasmesse le onde radio, e che lo spazio extra-terrestre è al di fuori dell'ordinario controllo degli Stati non ha impedito lo sviluppo di regole comuni le quali consentono la cooperazione internazionale nelle attività marittime, aeree, di telecomunicazione e satellitari[23]. Anche in questi casi si è di fronte ad attività che originano da un paese e sono destinate ad altri paesi, spesso attraverso[24] o sopra altri paesi, o su territori internazionali[25].

Il contenuto di regole esistenti[26] o future comprende una varietà di

to Internet Jurisdiction Based on Model of Harbors and the High Seas, in 29 *Int'l R.Law, Computers & Techn.* 266 (2015).

[23] W. Heintschel Von Heinegg, *Legal Implications etc*, cit. alla nt.7 definisce il ciber-spazio come un «global common» ovvero una *res communis omnium* (a p.9); and K. Ziolkowsi, *General Principles of International Law as Applicable in Cyberspace*, cit. alla nt.9, a p.167 qualifica «Internet come un'altra risorsa condivisa globalmente, il ciber-spazio come un altro spazio comune. Si potrebbero nutrire dei dubbi in ordine a tali qualificazioni: è discutibile che cavi sottomarini o satelliti per telecomunicazioni possano definirsi una res communis e si dovrebbe distinguere chiaramente l'elemento nel quale operano (l'acqua, l'aria, lo spazio extra-terrestre), la infrastruttura fisica, e l'attività che attraverso la infrastruttura viene condotta». La stessa A. va oltre proponendo, *de lege ferenda*, che Internet sia considerato«patrimonio comune dell'umanità» (a p. 181). Contro la teoria dei «global commons» v. P.W. Franzese, *Sovereignty in Cyberspace*, cit. alla nt.15 (pp. 14 ss.); B. Pirker, *Territorial Sovereignty and Integrity and the Challenges of Cyberspace*, cit. alla nt.16, a p. 194 s. suggerisce che «una titolarità fiduciaria [*trusteeship*] potrebbe essere una soluzione più adeguata per il futuro» (*ibidem*).

[24] Questo pone nuove questioni. Com'è noto il percorso che una comunicazione Internet prende dipende da una serie di fattori che in generale prescindono dalla volontà del mittente. Si possono applicare le regole internazionali consuetudinarie sul transito? Possono gli Stati esercitare un diritto sovrano di controllare (ed eventualmente bloccare e 'sequestrare') le comunicazioni che passano attraverso il proprio territorio? W. Heintschel Von Heinegg, *Legal Implications etc*, cit. alla nt.7 propone che il transito potrebbe essere limitato sulla base di «regole consuetudinarie o convenzionali di diritto internazionale» (a p. 11). Per alcune possibili soluzioni tecnologiche onde evitare il transito attraverso determinati stati v. T. Maurer et al., *Technological Sovereignty*, cit. alla nt.2 (a p. 58f)..

[25] Una ovvia problematica è quella dei cavi sottomarini analizzata da W. Heintschel Von Heinegg, *Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine Communications Cables under International Law*, in K. Ziolkowsi (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, 291 disponibile on-line alla pagina https://ccdcoe.org/publications/books/Peacetime-Regime.pdf [ultimo accesso 10.7.2016].

[26] Si discute fra gli studiosi di diritto internazionale se i tradizionali principi del diritto internazionale si applichino, e in che misura, al ciber-spazio. In senso affermativo v. K. Ziolkowsi, *General Principles of International Law as Applicable in Cyberspace*, cit. alla nt.9; E.T. Jensen, *Cyber Sovereignty: The Way Ahead*, 50 *Texas Int'l L.J.*. 275. Per una ulteriore ricognizione v. M.N. Schmitt, L. Vihul, *The Nature of International Law*

questioni: dagli standards tecnologici e la loro compatibilità alla identificazione dell'origine dei messaggi o lo stabilimento di coloro i quali forniscono servizi e contenuti.

Tuttavia la principale controversia – come risulta evidente dal caso *Schrems* – riguarda il contenuto di ciò che viene trasmesso attraverso le reti e quali attività possono, non possono e in quale maniera, essere svolte. Qualche indicazione potrebbe trarsi dal c.d. 'Internet Bill of Rights', ma questo copre solo una parte assai limitata di un quadro ben più ampio. Il governo di uno 'spazio' così grande come le reti globali richiede certamente l'individuazione e l'affermazione di diritti individuali[27], ma anche obblighi, doveri, norme dispositive, rimedi, regole per risolvere le controversie. Da questo punto di vista, da una prospettiva internazionale siamo ancora lontani da un assetto ancora embrionale.

La sentenza nel caso *Schrems* mette in luce l'esistenza di una controversia internazionale (chi controlla la rete e fissa le regole che governano le attività che vi si svolgono)[28] che può essere risolta solo attraverso i tipici strumenti del diritto internazionale[29].

Cyber Norms, Tallinn Paper n.5, CCD COE 2014 disponibile on-line alla pagina https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%20%205%20Schmitt%20and%20Vihul.pdf [ultimo accesso 10.7.2016].

[27] La prospettiva illustrata da M. Land, Toward an International Law of the Internet, 54 Harv. Int'l L. J. 393 (2013) fondata su una interpretazione espansiva dell'art.19 della Convenzione di New York del 1966 sui Diritti Civili e Politici appare influenzata da desiderata più che da una realistica (anche se rude) valutazione dell'attuale esercizio della sovranità degli stati sulle reti di telecomunicazione.

[28] Molte altre sono esposte da T. Maurer et al. , *Technological Sovereignty* , cit. alla nt.2 (a p. 63). Ad esse va aggiunta quella fra la Russia e la NATO sul diritto (ammesso che vi sia) applicabile alle c.d. ciber-guerre: v. A. Krutskikh, A. Streltsov, *International Law and the Problem of International Information Security*, in *International Affairs* n.6, 2014, 64 disponibile on-line alla pagina https://ccdcoe.org/sites/default/files/multimedia/pdf/International_Affairs_No6_2014_International_Law.pdf [ultimo accesso 10.7.2016]: «Alcuni esperti della NATO hanno sviluppato degli approcci per regolare scontri informatici (come il Tallinn Manual on the International Law Applicable to Cyber Warfare). La Russia segue una politica diametralmente opposta volta ad evitare scontri militari e politici nello spazio informatico» (a p. 75). E la risposta di W. Heintschel Von Heinegg, *International Law and International Information Security: A Response to Krutkikh and Streltsov*, Tallin Paper No.9, 2015 disponibile on-line alla pagina https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_09_2015.pdf [ultimo accesso 10.7.2016]

[29] V. P.W. Franzese, *Sovereignty in Cyberspace*, cit. alla nt. 15 a p. 32. Nello stesso senso J. Daskal, *The Un-Territoriality of Data*, cit. alla nt.14 a p. .

6. Le sedi internazionali per il governo delle reti digitali

La sede naturale per discutere e fissare regole comuni sembrerebbe essere l'Unione Internazionale per le Telecomunicazioni (ITU/UIT) considerata la sua esperienza di oltre un secolo e mezzo (è stata fondata nel 1865) e la diretta competenza sulle tematiche delle comunicazioni trans-nazionali[30]. Inoltre l'ITU prevede espressamente che soggetti privati (come le industrie) giochino un ruolo nel processo normativo, un profilo particolarmente importante considerando che la maggior parte dei soggetti impegnati nella determinazione del protocollo Internet e dei protocolli Internet-compatibili sono privati[31].

L'ITU ha prodotto un certo numero di decisioni ed accordi che riguardano Internet, ma esclusivamente su aspetti tecnici[32]. Bisogna però aggiungere che gli atti costitutivi e fondamentali dell'ITU non contengono disposizioni e procedure che riguardino la risoluzione delle controversie, il che da un lato riduce significativamente la forza vincolante delle sue risoluzioni ma al tempo stesso consente ai suoi membri di trovare sistemi alternativi per risolvere le dispute fra loro e dare vigore alla regolamentazione[33].

[30] In questo senso v. I. Walden. *International Telecommunications Law, the Internet and the Regulation of Cyberspace*, in K. Ziolkowsi (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, 261 disponibile on-line alla pagina https://ccdcoe.org/publications/books/Peacetime-Regime.pdf [ultimo accesso 10.7.2016].

[31] I. Walden. *International Telecommunications Law, the Internet and the Regulation of Cyberspace,* cit. alla nt. 20 , a p. 271.

[32] I. Walden. *International Telecommunications Law, the Internet and the Regulation of Cyberspace,* cit. alla nt. 20 a p. 264 evidenzia la complessità della distinzione fra regolazione tecnica di una infrastruttura e la regolazione dei contenuti di un servizio. Vi è tuttavia un notevole dibattito fra coloro che vorrebbero rafforzare il ruolo dell'ITU in questo campo, e quanti, come gli Stati Uniti e l'UE, hanno diversa visione (v. H. Tiirma-Klar, *Cyber Diplomacy: Agenda, Challenges and Mission*, in K. Ziolkowsi (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, 509, at p. 528 s.) disponibile on-line alla pagina https://ccdcoe.org/publications/books/Peacetime-Regime.pdf [ultimo accesso 10.7.2016]. See also D. P. Fidler, *Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations*, in 17 *Insights*, Issue 6, Feb. 2013 [papers of the American Society of International Law], disponibile on-line alla pagina https://www.asil.org/insights/volume/17/issue/6/internet-governance-and-international-law-controversy-concerning-revision [ultimo accesso 10.7.2016].

[33] I. Walden. *International Telecommunications Law, the Internet and the Regulation of Cyberspace,* cit. alla nt.20, a p. 276 : («Non vi è alcun meccanismo disponibile in caso di mancato rispetto». E' dubbio che l'alternativa sia il ricorso alla Corte Internazionale di Giustizia, suggerito da K. Ziolkowsi, *General Principles of International Law as Applicable*

L'occasione per un passo in questa direzione potrebbe essere rappresentati dai pendenti negoziati fra Unione Europea e Stati Uniti sul c.d. Trans-Atlantic Trade and Investment Partnership (TTIP)[34]. Alcuni commentatori hanno anche suggerito che la sentenza *Schrems* sarebbe un mezzo per rafforzare la posizione europea nel negoziare lo sviluppo dei servizi elettronici trans-atlantici i quali, comprensibilmente, sono uno dei principali impegni dell'amministrazione statunitense la quale apertamente sostiene le sue imprese in questo campo (Google, Apple, Facebook, Amazon etc.)[35].

in Cyberspace, cit. alla nt.9, a p. 175. Va peraltro osservato che nel caso di cavi sottomarini, regolati dalla Convenzione di Parigi del 1884 sulla Protezione dei cavi telegrafici sottomarini, e successivamente estesa alle comunicazioni telefoniche dalla Convenzione di Ginevra del 1958 sull'Alto Mare, le dispute potrebbero essere regolate sulla base delle Convenzione ONU del 1982 sul Diritto dei mari (v. W. Heintschel Von Heinegg, *Protecting Critical Submarine Cyber Infrastructure,* cit. alla nt.25 , a p. 308 s.).

[34] Per ragioni comprensibili la posizione dello US Trade Representative nel negoziato T-TIP è molto più chiaro su Internet v. https://ustr.gov/trade-agreements/free-trade-agreements/transatlantic-trade-and-investment-partnership-t-tip/t-tip-15 [ultimo accesso 10.7.2016]. La posizione dell'Unione si concentra di più sugli aspetti rispetto ai quali il divario con gli USA è meno forte, come nel caso del commercio elettronico v. http://trade.ec.europa.eu/doclib/docs/2015/january/tradoc_153009.pdf [ultimo accesso 10.7.2016].

[35] Nella misura in cui il negoziato TTIP si svolge nel generale quadro dell'OMC, una serie di elementi che sono stati delineati in quel contesto potrebbero essere opportunamente trasposti. V. I. Walden. *International Telecommunications Law, the Internet and the Regulation of Cyberspace,* cit. alla nt.20, alle pp. 278 ss (evidenziando, a p. 284 s., la maggiore efficacia delle procedure OMC per la risoluzione delle controversie). Opportunatamente parla di «market sovereignty» e di potenziali «market destroying measures» D.J.B. Svantesson, *The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on US Business,* 50 *Stan. J. Int'l L.*. 53 (2014). V. anche J.P. Trachchtman, *International Economic Law in the Cyber Arena*, in K. Ziolkowsi (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, 373 disponibile on-line alla pagina https://ccdcoe.org/publications/books/Peacetime-Regime.pdf [ultimo accesso 10.7.2016]; nonché S.A.Aaronson, *Why Trade Agreements are Not Setting Information Free: The Lost History and Reinvigorated Debate Over Cross-Border Data Flows, Human Rights and National Security*, disponibile on-line alla pagina http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2595809 [ultimo accesso 10.7.2016]; K. Eichensehr, *The Cyber-Law of Nations*, 103 *Geo. L.J.* 317 (2015) (sul ruolo dei soggetti privati nel governo di Internet).

7. Una visione d'insieme sulla 'sovranità digitale'

Il protocollo Intenet è una realtà non eludibile[36]. Evolverà tecnologicamente, economicamente, socialmente, trasformandosi in qualcosa di diverso, con un diverso nome. Ma concentrarsi esclusivamente su Internet rischia di guardare al problema da una prospettiva distorta. Le questioni attinenti alla sovranità forse, si spera, potranno trovare una soluzione guardando al quadro d'insieme, ed un approccio casuistico non è molto promettente: la protezione dei dati personali è intimamente connessa alle questioni di ciber-sicurezza; la tutela dei consumatori al commercio internazionale; le operazioni bancarie con la stabilità finanziaria; gli standards tecnologici con gli investimenti e il loro rendimento; l'applicazione della legge richiede indagini digitali transfrontaliere[37]. Il primo punto da individuare è individuare la sede dove negoziati seri possono essere iniziati; il secondo quello delle procedure da seguire nel processo decisionale[38]. Quindi si possono immaginare le varie tematiche, le quali sono tutte molto delicate da un punto di vista politico in quanto quasi tutte involgono i diritti dei singoli i quali utilizzano la messe di conoscenze e di opportunità offerte da Internet[39]. Da questo punto di vista si può osservare

[36] Non è questa la sede per analizzare i possibili sviluppi di Internet e le alternative, già esistenti, come il c.d. protocollo TOR (v. E.Çalışkan, T. Minárik, A-M Osula, *Technical and Legal Overview of the Tor Anonymity Network,* CCD COE, Tallinn 2015, disponibile on-line alla pagina https://cryptome.org/2015/07/TOR_Anonymity_Network.pdf [ultimo accesso 10.7.2016]. In ogni caso TOR è la dimostrazione che il protocollo Internet è solo uno dei tanti modi attraverso il quale è possibile accedere ed utilizzare una rete di telecomunicazione.

[37] Su quest'ultimo aspetto v. la Direttiva 41/2014 sull'Ordine europeo di indagine penale; nonchè il commento di A-M. Osula, *Accessing Extraterritorially Located Data: Options for States*, CCD COE – Nato Cooperative Cyber Defence Centre of Excellence, 2015 disponibile on-line alla pagina https://ccdcoe.org/sites/default/files/multimedia/pdf/Accessing%20extraterritorially%20located%20data%20options%20for%20States_Anna-Maria_Osula.pdf [ultimo accesso 10.7.2016]. V. inoltre l'art.32 della Convenzione di Budapest del 2001 sulla criminalità informatica.

[38] V. H. Tiirma-Klar, *Cyber Diplomacy: Agenda, Challenges and Mission*, e K. Ziolkowsi, *Confidence Building Measures for Cyberspace*, entrambi in K. Ziolkowsi (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, alle pp. 509 e 533 disponibile on-line alla pagina https://ccdcoe.org/publications/books/PeacetimeRegime.pdf [ultimo accesso 10.7.2016].

[39] Gli Stati Uniti hanno chiaramente espresso la loro posizione sui molti aspetti qui analizzati nel documento ufficiale della Casa Bianca «Prosperity, Security, and Openness in a Networked World», May 2011 disponibile on-line alla pagina https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

che numerose regole comuni possono essere estrapolate dal documento dell'OCSE del 2014 «Principles for Internet Policy-Making» nel quale sono indicate le risposte a molti dei principali problemi che interessano i paesi sviluppati e che richiedono cooperazione internazionale[40]. Occorre tuttavia evitare il pericolo che il dibattito su queste tematiche sia condotto e diretto da minoranze estremamente rumorose che hanno eletto Internet nella loro terra-di-nessuno che sarebbe sottratta all'impero della legge[41]. Non solo non si può sfuggire alla millenaria saggezza dell'*ibi societas ibi ius* (e le reti di telecomunicazione sono una parte, molto importante, delle società contemporanee) ma, ancor più importante, occorre evitare di creare nuovi tabù (Internet è al di fuori del diritto) che favoriscono un fenomeno opposto: l'utilizzo da parte degli Stati di pratiche occulte, segrete se non illegali[42].

[ultimo accesso 10.7.2016]. E nel luglio 2011 il Department of Defense ha pubblicato un documento intitolato «Strategy for Operating in Cyberspace» disponibile on-line alla pagina http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf [ultimo accesso 10.7.2016]; seguito, nel novembre 2011, dal «Cyberspace Policy Report» disponibile on-line alla pagina https://fas.org/irp/eprint/dod-cyber.pdf [ultimo accesso 10.7.2016].

[40] Disponibile on-line alla pagina http://www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf [ultimo accesso 10.7.2016] . L'indice elenca le seguenti questioni: «1.Promote and protect the global free flow of information. 2. Promote the open, distributed and interconnected nature of the Internet. 3. Promote investment and competition in high speed networks and services. 4. Promote and enable the cross-border delivery of services. 5. Encourage multi-stakeholder co-operation in policy development processes. 6. Foster voluntarily developed codes of conduct. 7. Develop capacities to bring publicly available, reliable data into the policy making process. 8. Ensure transparency, fair process, and accountability. 9. Strengthen consistency and effectiveness in privacy protection at a global level. 10. Maximise individual empowerment. 11. Promote creativity and innovation. 12. Limit Internet intermediary liability. 13. Encourage co-operation to promote Internet security. 14. Give appropriate priority to enforcement efforts». V. O. Pollicino, M. Bassini, *The Law of the Internet between Globalisation and Localisation*, in M. Maduro, K. Tuori, S. Sankari (a cura di), *Transnational Law: Rethinking European Law and Legal Thinking,* Cambridge UP*,* 2014, 346 (proponendo, a p. 372 s., il principio del mutuo riconoscimento).

[41] L'ovvio riferimento è al c.d. movimento «Anonymous» il quale opera sulla rete, spesso attraverso attacchi informatici nei confronti di coloro che individua come i propri avversari.

[42] Numerosi commentatori evidenziano che gli Stati hanno un interesse nel negare che le regole del diritto internazionale si applichino ad Internet: «Vi è una crescente evidenza che gli Stati si comportano come se vi fossero pochi, se non alcuno, limiti nello svolgimento di attività nel ciber-spazio» (P.A. Walker, *Law of the Horse to Law of the Submarine: The Future of State Behavior in Cyberspace*, in M. MAYBAUM, A-M. Osula, L. Lindstrom (a cura di), *7th International Conference on Cyber Conflict*, 2015 NATO

Abstract

The article analises the recent ECJ Schrems decision linking it to the 2014 Google Spain decision as an expression of EU sovereign powers on telecommunication networks. The article takes into account the various,competing, theories on 'sovereignty in cyber-space' pointing out ambiguities and misunderstandings (typically confusing the Internet protocol with an object of sovereign powers) and indicating the need for international cooperation in the appropriate fora (the ITU, the T-TIP negotiations) to set common rules which can enable free flow of communication and free provision of electronic services on transnational telecommunication networks.

CCD COE Publications at pp.97 and 104) (available on-line at https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2004%20Technological%20Sovereignity%20-%20Missing%20the%20Point.pdf [ultimo accesso 10.7.2016]. Analogamente v. P.W. Franzese, *Sovereignty in Cyberspace*, cit. alla nt.15 (a pp. 34 ss).