LA PROTEZIONE DEI DATI PERSONALI ED INFORMATICI NELL'ERA DELLA SORVEGLIANZA GLOBALE

Temi scelti

a cura di
Marcella Distefano

con la collaborazione di Marco Longobardo,
Livio Scaffidi Runchella e Federica Violi

Editoriale Scientifica

Progetto di ricerca finanziato da un progetto sull'argomento da parte dell'ILSA di Chicago, per il tramite dell'ILSA Chapter Messina e del CUMI

© Editoriale Scientifica srl giugno 2017
Via San Biagio dei Librai, 39
80138 Napoli
ISBN 978-88-9391-140-5

INDICE

SESSIONE TERZA:
PROFILI DI DIRITTO INTERNAZIONALE PRIVATO

ALBERTO ODDENINO*

LA VIOLAZIONE DI SISTEMI INFORMATICI CONTENENTI INFORMAZIONI RISERVATE COME ILLECITO INTERNAZIONALE: TRA DIMENSIONE INTERSTATUALE E TUTELA DEI DIRITTI UMANI

SOMMARIO: 1. Introduzione: sorveglianza, Internet e il necessario apporto di un approccio di diritto internazionale. – 2. La 'violazione di sistemi informatici contenenti informazioni riservate': elementi di descrizione nell'ardua ricerca di una *reductio ad unum.* – 3. I profili relativi all'elemento soggettivo e il problema dell'attribuzione di comportamenti posti in essere da o tramite soggetti privati. – 4. La ricostruzione dell'elemento oggettivo dell'illecito: il ruolo del diritto consuetudinario e delle norme convenzionali. – 5. S*egue*: l'elemento oggettivo oltre la dimensione strettamente interstatuale: la prospettiva di tutela dei diritti umani in relazione alla sorveglianza di massa. – 6. Conclusioni.

1. *Introduzione: sorveglianza, Internet e il necessario apporto di un approccio di diritto internazionale*

La configurazione della violazione di sistemi informatici come illecito internazionale è tema che ha acquisito una notevole rilevanza e una crescente centralità nel quadro del diritto internazionale contemporaneo. Le rivelazioni di Edward Snowden relative allo scandalo della *National Security Agency* (NSA)e l'emersione di un quadro ancor più sistematico di sorveglianza, mirata e massiva, condotto dai cd. *Five Eyes*[1], sono state il volano di tale rilevanza, che è suffragata, su un piano più generale, dalla definitiva presa della ribalta di Internet come mezzo di interconnessione dell'umanità del tempo presente, con la Rete delle reti, come è efficacemente definita, assurta ad emblema stesso della globalizzazione.

Come si vedrà, peraltro, tale immagine reticolare, ed in certa misura ubiqua, della Rete non può obliterare il legame con il territorio su cui essa si disloca ed insiste. Il che porta in primo piano una ineludibile relazione con la

* Professore associato di Diritto internazionale, Università di Torino.

[1] *FiveEyes* è un'alleanza di *intelligence* che lega Stati Uniti, Regno Unito, Australia, Canada e Nuova Zelanda, basata sulla cooperazione e la condivisione di segnali di comunicazione intercettati su scala globale. In tema si veda NYST, *The Five Eyes Fact Sheet,* in *Privacy International* (23 Novembre 2013, https://www.privacyinternational.org/blog/the-five-eyes-fact-sheet.

dimensione territoriale della sovranità statale, e sollecita un approccio specifico di diritto internazionale[2].Tecnicamente, infatti, Internet è in essenza il frutto di una 'universalizzazione' della interconnessione resa possibile dal protocollo IP eil suo funzionamento postula l'uso delle infrastrutture fisiche che formano i sistemi di telecomunicazione nazionali e che raccordano i medesimi a livello internazionale[3]. Per queste evidenti ragioni Internet è oggi campo di gioco della sorveglianza globale ma anche, al contempo, "territorio" fortemente conteso dalle diverse sfere di sovranità[4].

Ciò si riflette in modo particolare sul tema della sorveglianza. Il fenomeno, giova notare preliminarmente, incide sulle nostre società ben al di là di quanto si lega al fenomeno della sorveglianza di stato. Lo scenario è improntato a quella che è stata definita una 'nuova normalità' caratterizzata dalla più piena insicurezza dei nostri dati e dei nostri comportamenti in Rete[5]. I soggetti privati contribuiscono non meno di quelli pubblici a determinare tale scenario e

[2] In tema si vedano le considerazioni introduttive espresse in SCHMITT (ed. by), *Tallin Manual on the international law applicable to cyber warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence,* Cambridge, 2013, p. 2 ss.

Sulla prospettiva di una correlazione imprescindibile fra diritto e territorio anche in relazione alle nuove tecnologie, sia consentito rinviare a A. ODDENINO, *Law and Territory Happily ever After. Some Reflections on Globalization and International Law*, in DI STEFANO (a cura di), *A Lackland Law? Territory, Effectiveness and Jurisdiction in International and EU Law*, Torino, 2014, p. 115 ss.

[3] Un'interessante prospettiva sulla dimensione tecnica e fisica di Internet è offerta da DORMON, *How the Internet works: Submarine fibre, brains in Jar, and coaxialcables,* 24 maggio 2016 consultabile su http://arstechnica.com/information-technology/2016/05/how-the-internet-works-submarine-cables-data-centres-last-mile/.

[4] Ben lungi dalla concezione originaria come spazio di libertà tendenzialmente assoluta, che trovava nell'autoregolamentazione tecnica il solo modello normativo accettabile, la Rete, in ragione delle sue grandi potenzialità strategiche, sociali e commerciali, è oggetto di ambizioni di regolazione strutturale e contenutistica da parte di Stati, organizzazioni internazionali, organismi sovranazionali e, più in generale, soggetti portatori di rilevanti interessi economici, particolarmente quelli legati alla nuova frontiera del commercio e dello scambio dei dati.

In tema si veda, fra l'ampia letteratura, MUELLER, *Network and States. The Global Politics of Internet Governance*, MIT Press, 2010. Sia consentito rinviare anche a ODDENINO, *Il problema della governance internazionale della Rete*, in DURANTE, PAGALLO (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Torino, 2012, p. 45 ss.

[5] In merito è significativa la descrizione di questa evoluzione in termini di 'New Normal' in un Paper recentemente pubblicato dal *Center for Long-Time Cybersecurity* della Berkeley University (*Senario One. The New Normal,* 2017 reperibilesu https://cltc.berkeley.edu/scenario/scenario-one/) in cui si legge: «*Insecurity will become the starting assumption for every online interaction—not just for experts, but for everyone. Following years of escalating headlines about data breaches, internet users will operate with the belief that, sooner rather than later, their data will be stolen and their personal information broadcast*».

questo ha importanti ricadute di natura non solo giuridica ma anche economica e sociale[6].

Una ulteriore considerazione introduttiva deve essere dedicata alla circostanza che vede ogni discorso di regolazione di Internet e di tutela dei diritti nella dimensione *online* profondamente condizionato da assetti e rapporti di forza preesistenti e ampiamente consolidati: tali rapporti sono difficilmente sovvertibili e registrano una forte centralità degli USA nei meccanismi di *governance* e di sviluppo della Rete.

Ciò è riconducibile alla paternità statunitense nello originario sviluppo della Rete, che si è tradotto, fra l'altro, in un rapporto privilegiato con ICANN e IANA, soggetti deputati alla gestione del sistema dei nomi e dei numeri di Internet[7]. A un tale dato, per così dire genetico, fa da complemento la supremazia che gli USA hanno via via consolidato tanto in relazione all'aspetto della produzione di tecnologia di e per la telecomunicazione (Microsoft e Apple*in primis*, ma più in generale le aziende della *Silicon Valley*, che hanno costituito un distretto tecnologico senza pari nel mondo, capace di compendiare in sé le caratteristiche della *new economy* al punto da confondersi, in certa misura, con essa), quanto in relazione ai cosiddetti *Over the Top (OTT) Service Providers*, quali fra gli altri *Google*, *Facebook* e *Amazon*, colossi

[6] Sul tema, rilevantissimo da punto di vista degli operatori economici, di come il flusso, lo scambio e il commercio di enormi quantità di dati e metadati (associato alle capacità di calcolo e all'elaborazione, anche in chiave predittiva, da parte di algoritmi, nel quadro del fenomeno cd. *Big Data*) stia influendo in radice sul modello capitalistico contemporaneo, dando spazio allo sviluppo di quello che è stato definito efficacemente come 'capitalismo di sorveglianza', si veda ZUBOFF, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*in *Journal of Information Technology*, 2015, p. 75 e ss.

[7] Sul tema del rapporto privilegiato con gli USA, il riferimento d'obbligo va a GOLDSMITH, WU, *I padroni di Internet. L'illusione di un mondo senza confini*, Milano, 2006.

Sulle peculiarità dei meccanismi di *governance* e di sviluppo della Rete incentrati su ICANN si veda LAGRANGE, *L'Internet Corporation for Assigned Names and Numbers: un essai d'identification*, in *Revue générale de droit international public*, 2004, p. 305 ss., WEINBERG, *Non State Actors and Global InformalGovernance – The Case of Icann*, in CHRISTIANSEN, NEUHOLD (eds.) *International Handbook on Informal Governance*, Cheltenham, 2012, p. 292 ss.

Sull'evoluzione del sistema ICANN-IANA per la gestione dei nomi a dominio, e sulla sua attuale transizione verso un modello formalmente sottratto all'influenza statunitense si veda più di recente RUOTOLO, *Il sistema dei nomi a dominio alla luce di alcune recenti tendenze dell'ordinamento internazionale*, in *Il Diritto dell'Informazione e dell'Informatica*, 2016, p. 33 ss. Peraltro, la ricostruzione delle vicende della cosiddetta *IANA Transition* appare per certi profili controversa: dal punto di vista formale, la recentissima scadenza del contratto stipulato con il *Department of Commerce* segna la cessione del controllo su IANA da parte del governo statunitense ma non fa venire meno dubbi e riserve, come evidenziato fra l'altro da HILL, *Internet governance, multi-stakeholder models, and the IANA transition: shiningexample or dark side*, in *Journal of Cyber Policy*, 2016, disponibile su www.tandfonline.com.

della nuova economia che realizzano grazie alla Rete una strategia globale di massimizzazione del profitto.

A fronte di questo quadro, due dati strutturali restano ineludibili: il primo è la collocazione in territorio statunitense del *Root Server*, ossia della matrice unica e ultima degli indirizzi che compongono la Rete; il secondo è la possibilità di ciascuno Stato di operare un penetrante controllo, anche grazie all'intesa con i fornitori di tecnologie di rete e con le compagnie di telecomunicazione, sui segmenti nazionali della Rete. Dalla dinamica fra questi elementi discende una permanente tensione fra globalizzazione e balcanizzazione della Rete, e con tale dinamica si misura l'ambizione della stessa a mantenersi un tutto che sopravanza di molto la somma delle sue parti.

A tali riflessioni ci si riferisce quando si menziona una specifica dimensione geopolitica di Internet, ricordando con questa locuzione che quella che si gioca sulla Rete non è solo una partita per affermare una prevalenza economica: essa è una vera contesa di potere, nella sua accezione più ampia e totalizzante[8].

Si tratta di una considerazione particolarmente calzante se ci si riferisce al tema della sorveglianza e della tutela dei dati e della *privacy* e a temi, come quello dei *Big Data* e del governo degli algoritmi, che, al di là di un intuitivo utilizzo volto in particolare alla profilazione commerciale, sono al contempo straordinari strumenti di controllo, suscettibili di plasmare in radice non solo gli assetti e gli equilibri delle nostre abitudini sociali, ma l'essenza stessa del nostro modello economico e delle nostre democrazie.

È alla luce di queste considerazioni preliminari sul legame fra Internet e

[8] È evidente come la contesa per il controllo della struttura sia propedeutica al controllo dei contenuti: la possibilità di realizzare una penetrante sorveglianza e una raccolta sistematica di informazioni strategiche, anche e soprattutto in dimensione internazionale, non può che essere vista come espressione qualificata di un tale disegno. In tema si veda DE NARDIS, *The Global War for Internet Governance*, Yale, 2014.

Quanto la contesa fra gli stati sia aspra ed aperta è risultato con particolare evidenza anche in occasione della recente disputa relativa alla riforma delle *International Telecommunications Regulations* dell'ITU: essa ha visto, nella Conferenza di Dubai del 2012, lo scontro fra visioni e pretese contrapposte, segnando una profonda lacerazione fra gli stati solidali con la posizione volta al sostanziale mantenimento dello *status quo*, espressa dagli USA, e quelli che, come Cina e Russia in particolare, in una logica geopolitica di contropotere, hanno tentato di affermare una visione alternativa, sulla base di dichiarate esigenze di cybersicurezza. Sul punto si veda FIEDLER,*Internet Governance and International Law: The Controversy concerning Revision of the International Telecommunication Regulations*, in *ASIL Insights*, 6, 2013, <www.asil.org/pdfs/insights/insight130207.pdf>.

In tema sia consentito rinviare anche a ODDENINO, *Diritti individuali, sicurezza informatica e accesso della conoscenza in Rete: la revisione delle* International Telecommunication Regulations *dell'ITU*, in *Diritti umani e diritto internazionale*, 2013, p. 525 ss.

sovranità statali che si può apprezzare l'importanza di un approccio, e di uno specifico apporto, del diritto internazionale al tema, complesso e multiforme, della regolazione di Internet[9]. Questo, se è vero già su un piano generale, diviene particolarmente evidentese si fa riferimento specifico alla attività di controllo e sorveglianza che può essere svolta attraverso la Rete.

Tassello fondamentale di una riflessione internazionalistica che si concentri sulla Rete, e sulle esigenze di tutela dei diritti fondamentali nella dimensione *online*, è proprio la possibilità di ricostruire la violazione di sistemi informatici come illecito internazionale dello Stato. Si tratta di una ricostruzione non scontata, per i motivi che si esamineranno, con particolare, ma non esclusivo, riferimento all'elemento della antigiuridicità e con particolare delicatezza in relazione a condotte che non presentino profili di extraterritorialità.

Nel presente contributo si muoverà pertanto da un'opera di inquadramento e di ricerca definitoria e tassonomica, funzionale alla ricostruzione dei confini categoriali dell'illecito, dal punto di vista tanto dell'elemento soggettivo quanto di quello oggettivo, per poi svolgere qualche considerazione più generale sul legame fra dimensione strettamente interstatuale dell'illecito ed esigenze di protezione di diritti fondamentali, con particolare riferimento alla *privacy* e alla tutela dei dati personali nel contesto dei meccanismi di sorveglianza, anche massiva, che caratterizzano la nostra epoca. L'interrogativo che si porrà in conclusione riguarda i termini del rapporto di complementarietà fra queste due dimensioni, nonché la loro adeguatezza rispetto alle sfide poste da un fenomeno sempre più totalizzante.

2. *La 'violazione di sistemi informatici contenenti informazioni riservate': elementi di descrizione nell'ardua ricerca di una* reductio ad unum

Da un punto di vista generale, occorre muovere dalla premessa, finanche scontata, che qualunque analisi normativa presuppone una condivisa comprensione di alcune categorie che vanno a comporre la fattispecie esaminata. In particolare, è il concetto di 'violazione di sistemi informatici contenenti informazioni riservate'a dover essere vagliato e ben definito, dal momento che esso è funzionale a perimetrare lo stesso campo di applicazione dell'illecito che qui ci occupa, provvedendo al contempo a escludere dalla presente analisi alcuni temi ad essa connessi ma non pienamente sovrapponibili. In questo

[9] Una specificità internazionalistica dell'indagine è coltivata nella dottrina italiana in ODDENINO, *La governance di Internet fra autoregolazione, sovranità statale e diritto internazionale*, Torino, 2008 e in RUOTOLO, *Internet-ional Law. Profili di diritto internazionale pubblico della Rete*, Bari, 2012.

senso, deve essere interpretata l'introduzione di alcune fondamentali distinzioni, e il tentativo, non sempre agevole, di approdare ad una *reductio ad unum* delle fattispecie coinvolte nell'analisi[10].

In relazione alla nozione di 'violazione', si possono operare distinzioni che hanno a che vedere con le modalità con cui essa è realizzata. In primo luogo, vi è da considerare l'accesso ai sistemi informatici che avviene mediante la violazione dei meccanismi di sicurezza dei medesimi. La categorizzazione è quella dell'accesso abusivo a sistema informatico, contenuta all'art. 2 della Convenzione di Budapest (*Illegal Access*) sulla criminalità informatica, la quale, pur volta a diversi obiettivi fornisce utili elementi definitori[11].

Diverso è il caso della intercettazione di una comunicazione in corso. Non si tratta, in questo caso, di una vera e propria violazione di sistema, identificabile, perlopiù, con una banca dati: si tratta, al contrario, dell'utilizzo di strumenti di intercettazione che intervengono sulla struttura che supporta la comunicazione stessa. Anche questa è una dimensione che presenta profili abusivi, e il riferimento può andare all'art. 3 della Convenzione di Budapest (*Illegal Interception*),[12] ma è evidente che l'aspetto dell'abusività può anche essere più sfumato, e essere invece maggiormente rilevante il profilo della interazione con i dati (il riferimento potrà anche andare in questo senso all'art. 4 della medesima Convenzione[13], dedicato alla *Data Interference*[14]).

[10] Preliminarmente occorre precisare che resta al di fuori del presente campo di indagine l'attività di controllo e sorveglianza che avviene al di fuori del cyberspazio e dunque senza il tramite del mezzo informatico, seppure con l'utilizzo di sistemi di captazione audio e video ad elevato gradiente tecnologico.

[11] *Council of Europe*, ETS n. 185, *Convention on Cyber Crime*, Budapest, 23 novembre 2001, art. 2, ai sensi del quale l'accesso abusive dovrebbe consistere in «*an offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system*». Il riferimento alla Convenzione di Budapest ha in questa sede il valore di fornire elementi funzionali alla costruzione di una tassonomia, e non implica evidentemente una estensione alla dimensione dell'illecito interstatuale dell'applicabilità della Convenzione, che nasce, come noto, con l'intento di introdurre negli Stati contraenti fattispecie condivise volte alla criminalizzazione, nei rispettivi diritti nazionali, di condotte informatiche.

[12] *Council of Europe*, ETS n. 185, *Convention on Cyber Crime*, Budapest, 23 novembre 2001, art. 3, che contiene la seguente definizione: « *the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data*».

[13] *Council of Europe*, ETS n. 185, *Convention on Cyber Crime*, Budapest, 23 novembre 2001, art. 4, che offre una definizione certamente ampia di *interference*, la quale può essere costituita da «*damaging, deletion, deterioration, alteration or suppression of computer data without right*».

[14] Rispetto all'intercettazione, è importante tenere costantemente presente come la struttura fisica della Rete, come si riferiva nel paragrafo introduttivo, non è affatto omogenea e si regge

Un secondo livello di analisi muove dal legame fra la articolazione fisica della Rete e la possibilità di intervenire su di essa con intenti distruttivi. Questo non fa che confermare la lettura geopolitica degli assetti della Rete cui si faceva cenno e conduce a confrontarsi con la categoria dell'attacco informatico. Essa spesso si presenta con una certa contiguità, e continuità, rispetto alla fattispecie dell'accesso abusivo, che spesso può portare con sé strumenti non solo di *intelligence*, ma anche distruttivi o modificativi del sistema informatico.

Non è intento di questo contributo quello di entrare nel merito dell'ampio dibattito rispetto alle cd. *cyberoperations*, e al connesso tema dell'uso della forza informatica,[15] ma ciò che appare evidente è che in molti rispetti tutte le distinzioni che si sono appena tracciate presentano non poche zone grigie, ed è frequente ravvisare nella pratica situazioni ibride in cui all'aspetto dell'accesso abusivo si accompagnano intenti modificativi o anche distruttivi. Decisiva in questo senso è la presenza, per la configurabilità dell'attacco informatico, di un elemento di danno non reversibile, ma ciò spesso non è risolutivo, dal momento che i labili confini fra accesso, intercettazione e attacco discendono dalla operatività in modalità mista dello stesso mezzo tecnologico impiegato. Esemplare in questo senso è stato il caso *Stuxnet* in cui uno stesso virus informatico svolgeva al contempo funzioni di *spyware* e *malware*, e perseguiva pertanto obiettivi congiunti tanto di spionaggio quanto di modifica e sabotaggio del sistema informatico di una centrale nucleare iraniana[16]. Si tratta

invece su dorsali, snodi e cavi strategici attraverso cui passano enormi quantità di dati, instradati da potenti *routers*. Si tratta di una struttura che rende possibile situare su snodi strategici i mezzi di intercettazione e che rende questa attività evidentemente più agevole per gli stati che ospitano detti snodi sul proprio territorio. È questa una circostanza che, per le ragioni che si menzionavano nel paragrafo introduttivo in relazione allo sviluppo storico della struttura fisica della Rete, pone gli Stati Uniti in una posizione di favore nella intercettazione di comunicazioni in corso: essi possono infatti, più di ogni altro stato, operare prescindendo da una azione che presenti chiari profili di extraterritorialità. All'aspetto della struttura fisica, e in particolare della dorsale atlantica, si aggiunge, come si diceva, il dato, di per sé tutt'altro che trascurabile, della presenza sul territorio statunitense del cosiddetto *root server* (o server A), che rappresenta la radice e la matrice fondamentale di tutto il sistema dei nomi e dei numeri di internet, ossia l'ossatura degli indirizzi che compongono la struttura geografica della Rete e la garanzia di unità del sistema.

[15] Su cui si veda ampiamente ROSCINI, *Cyber operations and the use of force in international law*, Oxford, 2014.

[16] Diversi autori si sono espressi nel senso di considerare il caso *Stuxnet* come uso della forza ai sensi dell'art. 2 par. 4 della Carta delle Nazioni Unite. Per tutti vedi BUCHAN, *Cyberattacks: unlawful uses of force or prohibited intervention?* in *Journal of Conflict and Security Law*, 2012, pp.219-221. Per una ricostruzione della vicenda e delle sue implicazioni geopolitiche si

di un caso che revoca in dubbio, sul piano pratico e operativo, la nettezza di una distinzione, quella fra *cyber attack* e *cyber exploitation*[17], che è invece comunemente richiamata in dottrina come vero postulato normativo del sistema, che fonda un dualismo di regime[18].

Distinzione fondamentale, e strettamente legata a quella appena menzionata, è quella relativa al contesto in cui la violazione si realizza, e riguarda la tenuta della condotta in tempo di pace[19] o in costanza di un conflitto armato.[20] Si tratta di una distinzione che deve essere letta congiuntamente alla presenza o meno di un intento distruttivo cui l'azione è tesa. Si tratta di due prospettive che si completano a vicenda e la cui analisi esula dall'economia del presente lavoro: dal momento che coinvolgono plessi normativi differenti e implicano il confronto con il tema della legittima difesa e, più in generale, con il tema delle conseguenze dell'illecito, dai quali si è scelto necessariamente di prescindere[21].

Ne discende che, introdotte e individuate le distinzioni fra violazione in tempo di pace e in tempo di guerra e fra violazioni implicanti o non implicanti l'uso di quella che si può definire la forza bellica, si limiterà lo scopo della definizione di 'violazione di sistemi di informazioni riservate', e con esso la portata della presente indagine, a violazioni che avvengano in tempo di pace e prive di intento e portata distruttiva.

Un ulteriore elemento di distinzione, accanto alle modalità e al tempo in cui la violazione si realizza, ha a che vedere, congiuntamente, con le finalità della medesima e con il suo oggetto.

Occorre notare come le finalità della violazione possano essere le più varie, e come esse non siano sempre né esplicite né pienamente dichiarate o dichiarabili. In primo luogo vi sono le esigenze della sicurezza nazionale e internazionale, con particolare riferimento alle minacce terroristiche che hanno as-

rinvia a VALERIANO, MANESS, *Cyber war versus cyber reality: cyber conflict in the international system*, Oxford, 2015, p. 138 ss.

[17] Rilevante in proposito è la definizione che gli Stati Uniti danno di *Cyber network exploitation operations*, in particolare si veda la definizione contenuta in US National Military Strategy for Cyberspace Operations, 2006, punto GL-1, secondo la quale le operazioni di *network exploitations* sarebbero quelle finalizzate a «*enabling operations and intelligence collection to gather data from target or adversary automated information systems or network*s».

[18] In tema si veda fra gli altri LIN, *Cyber conflicts and international humanitarian law*, in *International Review of the Red Cross*, 2012, pp. 518-519.

[19] In tema si veda già EDMONDSON, *Espionage in Transnational Law*, in *Vanderbilt Journal of Transnational Law*, 1972, p. 434. Sul punto si rinvia altresì al contributo di M. LONGOBARDO nel presente volume.

[20] Sul punto DINNIS, *Cyber warfare and the laws of war*, Cambridge, 2012, p. 117 ss.

[21] Su questi aspetti cfr. ROSCINI, *Cyber operations and the use of force*, cit., p. 44 ss.; si veda inoltre TSAGOURIAS, *Cyber-attacks, self-defence and the problem of attribution*, in *Journal of Conflict and Security Law*, 2012, p. 229 ss.

sunto in tempi recenti una dimensione sempre più capillare e radicata all'interno del mondo occidentale. Il dibattito, attualissimo, sul ricorso ad uno stato di eccezione permanente è a tale proposito emblematico, ed è suscettibile di mutare in modo irreversibile il bilanciamento fra esigenze di sicurezza e tutela della sfera di libertà individuale[22].

In secondo luogo si possono individuare esigenze di puntuale repressione criminale, legate alla ricerca di prove finalizzate alla piena ed efficiente applicazione del sistema penalistico di uno stato. Si tratta di ipotesi di intervento mirato che suscitano minori riserve dal punto di vista della tutela dei diritti, dal momento che si reggono sul presupposto di una autorizzazione di organi giudiziari e su quello del controllo e della revisione, secondo i vari sistemi di *judicial review*[23].

Altre finalità hanno invece a che vedere con l'acquisizione di meno dichiarabili vantaggi competitivi, che coprono l'ampio spettro che va dai profili di *intelligence* di aspetti strategici all'appropriazione di segreti industriali. Anche in relazione a queste distinzioni non può che ripetersi quanto già si affermava rispetto alla frequente incertezza di precise linee di discrimine.

Il profilo legato alla finalità condiziona poi potentemente il tema dell'oggetto della violazione. In alcuni casi, e in particolare nell'ambito della violazione legata ad esigenze di repressione penale, l'oggetto della condotta è mirato e ben predeterminato, e lo si può pertanto descrivere come 'individualizzato'.

Ben altro scenario si presenta allorché l'accesso, ma soprattutto l'intercettazione, avvenga con portata massiva e indiscriminata (*mass surveillance, bulk interception*) e riguardi non solo dati ma anche metadati, ossia

[22] Si pensi ai numerosi casi in cui l'accesso ai dati personali è realizzato nell'ambito di programmi di c.d. sorveglianza di massa (su cui v. *infra)*, spesso giustificati proprio sulla base di esigenze connesse alla lotta al terrorismo internazionale. Sul tema della complessa relazione fra terrorismo internazionale e tutela dei dati si veda ampiamente NINO, *Terrorismo internazionale, privacy e protezione dei dati personali*, Napoli, 2012.

Sull'evoluzione dello spionaggio tradizionale nel diritto internazionale si veda KIRCHNER, *Beyond privacy rights: crossborder cyber-espionage and international law*, in *J. Marshall Journal of Information Technology and Privacy Law*, 2014, p. 369 ss. Sulla prassi più recente si veda RUBINSTEIN, NOJEIM, LEE, *Systematic government access to personal data: a comparative analysis*, in *International Data Privacy Law*, 2014, p. 96 ss.

[23] Si tratta di garanzie cui anche la Corte europea dei diritti dell'uomo ha subordinato la legittimità di tali tipi di interferenze. Si vedano come significative, recentemente, Corte europea dei diritti dell'uomo, *Zakharov v. Russia*, ricorso n. 47143/06, sentenza del 4 dicembre 2015, par. 264; Corte europea dei diritti dell'uomo, *Szabò and Vissy v. Hungary*, ricorso n. 317138/14, sentenza del 12 gennaio 2016, par. 57 ss. Si vedano altresì le analoghe conclusioni della Corte di giustizia dell'Unione europea, causa C-362/14, *Schrems c. Data ProtectionCommissioner*, sentenza del 6 ottobre 2015, parr. 91-95.

l'ampia massa di dati relativi alla navigazione in Internet. Le capacità computazionali che sono state sviluppate, attraverso sempre più raffinati algoritmi e attraverso una crescente capacità combinatoria e di aggregazione (*data mining*) di enormi quantità di dati (ciò che va sotto l'etichetta del fenomeno c.d. *Big Data*), conducono a configurare una capacità di intrusione nella sfera della vita privata degli individui che porta a modificare in modo irreversibile il bilanciamento fra esigenze di dichiarata sicurezza e sfera privata. E' infatti evidente che in questi casi si è in presenza di un sovvertimento del paradigma del controllo, con conseguente generalizzazione dell'eccezione costituita dalla compressione della sfera di libertà privata[24]. Il che comporta l'abbandono in radice di ogni serio intento di contemperamento dei valori in gioco, dal momento che ogni tentativo di bilanciare *privacy* e sicurezza postula una considerazione e una calibratura individualizzata della misura, e non, invece, l'attribuzione a priori di una sorta di carta bianca volta a legittimare il pubblico potere rispetto a condotte di sorveglianza massiva e indiscriminata[25].

Da ultimo, è assai rilevante analizzare la dimensione spaziale della violazione, ossia la sua portata territoriale. Da questo punto di vista occorre distinguere fra almeno tre diverse fattispecie: l'accesso che avviene in modo chiaramente e schiettamente extraterritoriale, l'accesso o l'intercettazione che presenta una portata solo infra-territoriale, e infine la cosiddetta 'intercettazione transnazionale'[26]. L'elemento della extraterritorialità è incontestabilmente presente solo nella prima fattispecie, mentre tanto nella seconda quanto nella terza ipotesi l'extraterritorialità ha certo a che vedere con la provenienza o la destinazione dei dati, ma non caratterizza la condotta di accesso o intercettazione come tale. Si tratta, pertanto, di fattispecie in cui la ricostruzione in termini di illecito internazionale interstatuale appare più delicata proprio perché manca l'elemento della diretta interferenza, ed ingerenza, rispetto alla sfera di

[24] Cfr. *UN Human Rights Council*, Doc. A/69/397, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, 23 settembre 2014, par. 51 ss.

[25] Si tratta in cui evidentemente viene in rilievo la peraltro discussa applicabilità delle norme internazionali a tutela dei diritti fondamentali. Sul punto, su cui si tornerà anche nel paragrafo 5, si veda MILANOVIC, *Human rights treaties and Foreign Surveillance: privacy in the digital age*, in *Harvard International Law Journal*, 2015, p. 81 ss.

[26] Il primo caso si verifica quando lo Stato A accede abusivamente al sistema di dati e informazioni che è situato sul territorio dello Stato B; il secondo caso si dà quando lo Stato A accede a dati dello Stato B, o che sono relativi allo Stato B, o più in generale a suoi cittadini, ma ciò avviene sul territorio dello Stato A perché tali dati sono ivi disponibili o perché sono qui conservati o perché sono in transito; il terzo caso si verifica infine quando lo Stato A intercetti sul proprio territorio una comunicazione in transito fra il territorio dello Stato B e dello Stato C.

sovranità territoriale di altri stati[27]. Il discorso si pone differentemente in relazione al tema della violazione di diritti fondamentali, in cui l'elemento della extraterritorialità gioca un ruolo essenziale ed è posto al centro di un importante dibattito[28]. Come si vedrà trattando dell'elemento oggettivo, il nodo di questa problematica sta nell'individuare la portata delle norme convenzionali poste a tutela della riservatezza, e vagliare in che misura esse possano applicarsi a condotte che lo stato tiene extraterritorialmente, anche a prescindere dalla dimostrazione, che risulterebbe allo stato attuale del diritto internazionale assai ardua, che esse hanno acquisito natura consuetudinaria ed hanno pertanto portata generale. A questo proposito, l'elemento della extraterritorialità rivela alcuni profili potenzialmente paradossali: se esso sembra necessario a configurare l'illecito in dimensione interstatuale, per quella che si è descritta come l'indebita ingerenza nella sfera di sovranità di un altro stato, esso al contempo pone le basi per argomentare in favore dell'esclusione dalle garanzie di diritti fondamentali[29]. Si tratta di una circostanza che, come si vedrà più puntualmente nel prosieguo, evidenzia la necessità di un approccio che completi reciprocamente le prospettive di ricostruzione dell'illecito interstatuale e quelle di tutela dei diritti individuali.

[27] In generale sulle difficoltà legate all'identificazione di spazi riservati alla sovranità statale rispetto al cyberspazio si veda DE LA CHAPELLE, FEHLINGER, *Jurisdiction on the internet: from legal arms race to transnational cooperation*, in *Global Commission on Internet Governance Paper Series* n. 28, aprile 2016.

[28] In tema si veda MILANOVIC, *Human rights treaties and Foreign Surveillance cit.* in particolare p. 118 ss., ove si configura un modello in cui coesistono una obbligazione negativa, ossia di rispetto dei diritti fondamentali nelle condotte ascrivibili allo stato, che avrebbe portata anche extraterritoriale e una obbligazione positiva, che risulta più incisiva per contenuto, perché comporta un dovere di prevenzione della violazione anche da parte di soggetti non statuali, ma che ha necessariamente una applicazione territoriale limitata allo spazio che è sottoposto al controllo statale.

[29] Tale profilo si è reso evidente in un caso recente in cui il giudice inglese ha escluso l'applicabilità della Convenzione europea dei diritti dell'uomo a programmi di sorveglianza condotti dal Regno Unito al di fuori del proprio territorio. Si veda*UKInvestigatory Powers Tribunal, Human Rights Watch and others v. Secretary of State for the Foreign and Commonwealth Office*, Sentenza del 15 aprile 2016, su cui RAIBLE, *Human Rights Watch v. Secretary of State for the Foreign and Commonwealth Office: Victim status, extraterritoriality and the search for principled reasoning* in *Modern Law Review,* 2017, p. 510 ss. Si segnala che la medesima delicata questione si trova ora all'esame della stessa Corte EDU.

3. *I profili relativi all'elemento soggettivo e il problema dell'attribuzione di comportamenti posti in essere da o tramite soggetti privati*

Alla luce delle distinzioni e delle categorie introdotte, e sul presupposto di delimitare, sulla base delle medesime, l'indagine sulla violazione di sistemi di informazioni riservate a condotte tenute in tempo di pace e prive di portata distruttiva, è possibile volgere all'analisi della sussistenza degli elementi costitutivi dell'illecito.

Il profilo soggettivo dell'illecito, ossia l'attribuzione della condotta illecita ad un soggetto statale[30], è prevalentemente affrontato in dottrina in relazione alla fattispecie del *cyber* attacco, ma deve in questa sede necessariamente essere declinato nella dimensione più contenuta determinata dallo scopo dell'indagine.

Si tratta di un profilo che pone poche difficoltà nel caso in cui la condotta in esame (prescindendo in questa sede se sia essa di accesso abusivo, e dotata o meno di elemento coercitivo, o di semplice intercettazione di un flusso di dati con obiettivo di sorveglianza) sia realizzata da agenzie di stato, o sia comunque direttamente riconducibile all'azione di organi di stato, per i quali vige il nesso di identificazione organica[31].

Il tema si pone in termini differenti, anche per i problemi di attribuzione tecnica, nel caso dell'organo di fatto, di cui all'art. 5 del Progetto[32]. È un tema delicato della nostra indagine perché riguarda l'ipotesi della vigilanza effettuata dallo stato per il tramite di soggetti privati[33]. La prassi più recente dimostra

[30] Per una ricostruzione, sintetica, dei principali approcci in ordine alla ricostruzione del fenomeno dell'attribuzione si veda SPINEDI, *Responsabilità internazionale*, in *Enciclopedia Giuridica*, vol. XXVII, Roma, 1985, p. 3 e CONDORELLI, *L'imputation à l'Etat d'un fait internationalement illicite: solutions classiques et nouvelles tendences*, in *Recueil des Cours de l'Académie de Droit International de la Haye*, 1984. Più recentemente si veda anche MESSINEO, *Attribution of conduct*, in NOLLKAEMPER, PLAKOKEFALOS (eds.), *Principles of Shared Responsibility in International Law*, Cambridge, 2014.

[31] Si tratta di fattispecie che ricadono nel campo di applicazione dell'art. 4 del Progetto di articoli sulla responsabilità dello Stato della CDI, di seguito semplicemente il 'Progetto'.

[32] Sugli aspetti tecnici dell'attribuzione di *cyber operations* cfr. RID, BUCHANAN, *Attributing cyber attacks*, in *Journal of Strategic Studies*, 2015, p. 4 ss. Le disposizioni di cui all'art. 4 del Progetto di articoli dovrebbero però essere coordinate con la Rule 7 del *Tallin Manual*, che, in via cautelativa, dispone che «*the mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State, but is an indication that the State in question is associated with the operation*». Con riguardo, soprattutto, al dibattito sul ruolo del diritto interno dei singoli Stati nella definizione di 'organo', si veda PALCHETTI, *L'organo di fatto dello Stato nel diritto internazionale*, Milano, 2007, in particolare pp. 1-20.

[33] Sul problema, in generale, si veda BARTOLINI, *Il concetto di "controllo" sulle attività di*

proprio la tendenza degli stati ad imporre per legge obblighi di messa a disposizione da parte di *Internet Service Providers* (ISP) dei dati dai medesimi custoditi in ragione della propria attività e dei contratti con gli utenti[34].

Prassi recente come quella evidenziata nel caso *Microsoft*, relativo alla richiesta di dati detenuti anche extraterritorialmente, in particolare su territorio irlandese, dimostrano l'entità e la delicatezza di questo profilo del problema[35]. Si tratta a bene vedere di situazioni in cui il privato non solo è autorizzato dalla legge ma è obbligato dalla medesima a tenere un determinato comportamento, di portata extraterritoriale e suscettibile di concretizzare una condotta internazionalmente illecita sotto il profilo oggettivo: esso sotto questo profilo rientrerebbe senza dubbio nel campo di applicazione dell'art. 5 del Progetto, nella sua interpretazione come criterio non strutturale ma funzionale, e dunque suscettibile di coprire anche i comportamenti tenuti da soggetti privati[36]. Ciò che però rileva ai fini di questo tipo di attribuzione è che le funzioni siano tipiche della potestà pubblica del governo statale[37], e ciò deve necessariamente riverberarsi anche sulla natura dell'atto posto in essere, che deve essere in certa misura almeno riconducibile alla funzione di governo dello Stato[38].

individui quale presupposto della responsabilità dello Stato, in SPINEDI, GIANELLI, ALAIMO (a cura di), *La codificazione della responsabilità internazionale degli Stati alla prova dei fatti. Problemi e spunti di riflessione*, Milano 2007, p. 25 ss., in particolare p. 26-27 e p. 36.

[34] In proposito, è ancora una volta la posizione degli Stati Uniti ad essere paradigmatica, ed esemplificativa una volta di più della già menzionata prevalenza tecnologica che discende dal fatto che virtualmente tutte le società che dominano la *new economy* hanno la propria sede principale negli USA e sono pertanto soggette alle leggi statunitensi.

[35] Il caso si è recentemente concluso con una significativa pronuncia a favore di Microsoft, fondata sulla impossibilità di applicare un mandato di perquisizione a dati posseduti da Microsoft nel territorio di un altro Stato. Cfr. *US Court of Appeals*, *2nd Circuit*, *Microsoft Corporations v. United States of America*, 14 luglio 2016.

Come variante del caso può essere interpretata anche la vicenda del caso Apple FBI, che è nato dalla richiesta dell'agenzia governativa di accedere a un dispositivo *smartphone* per ragioni di antiterrorismo, ma secondo una modalità che avrebbe surrettiziamente creato, attraverso una *backdoor* tecnologica permanente, una possibilità generale e permanente di accesso e sorveglianza suscettibile di esplicarsi, attraverso il dispositivo, anche in dimensione extraterritoriale.

[36] In tema CRAWFORD, *State Responsibility. The General Part*, Cambridge, 2014, p. 127.

[37] Per questo il caso tipicamente evocato è quello delle *Private military and security companies*. In tema si veda TONKIN, *State control over private military and security companies in armed conflict*, Cambridge, 2011, p. 101 ss.

[38] Il corollario di questa impostazione è che solo se l'atto non avrebbe potuto essere compiuto dal privato che con l'autorizzazione dello Stato, esso potrà essere ricondotto al campo di applicazione dell'art. 5 del Progetto. Per questo si può ritenere che si rientri nella fattispecie di cui all'art. 5 nel caso del tradizionale spionaggio diplomatico, con i dati intercettati da privati su mandato dello Stato, non essendo ipotizzabile che queste siano attività che la società possa svolgere nel quadro delle sue ordinarie attività economiche.

Sotto questo profilo, l'utilizzo del criterio di attribuzione di cui all'art. 5 del Progetto può rivelarsi più delicato, perché è evidente come, di per sé, la raccolta di dati da parte degli ISP rientri nella normale loro sfera di attività, e ciò si svolge sulla base di precise disposizioni contrattuali con gli utenti dei servizi e certamente prescinde in sé dalla presenza o assenza di una autorizzazione nonché dall'esistenza di un vero e proprio obbligo di matrice statale.

Ciò, oltre ad evidenziare la difficoltà concreta di distinguere in modo generale fra finalità privatistiche e pubblicistiche nel trattamento, anche extraterritoriale, dei dati, suggerisce di vagliare la possibilità di ricorrere al diverso criterio di attribuzione di cui all'art. 8 del Progetto. Tale disposizione, come è noto, identifica due diverse ipotesi: quella del soggetto che agisce "su istruzione" dello Stato e il soggetto che agisce sotto la direzione o il controllo dello Stato. Più interessante, ai nostri fini, appare la prima ipotesi, che sussiste quando lo Stato dia istruzione ad un soggetto privato perché questo tenga un determinato comportamento in sua vece[39]. Attraverso questa impostazione è altresì possibile tracciare una linea di confine con l'altro criterio dell'art. 8, quello del controllo effettivo, che presenta soglie probatorie e applicative che possono rivelarsi ardue da soddisfare nelle fattispecie in esame.

In definitiva, il caso in cui lo Stato abbia obbligato, normativamente o amministrativamente, soggetti privati stabiliti sul suo territorio a raccogliere, in virtù della loro stessa attività economica, ma per suo conto ed abusivamente, dati presso sistemi informatici collocati extraterritorialmente, la violazione sarà attribuibile allo Stato laddove, in virtù dell'elemento delle istruzioni, sia provato il collegamento previsto dall'art. 8.

Una prospettiva ancora differente è quella di valutare la responsabilità dello Stato per attività poste in essere da soggetti privati senza mandato dello stato e per finalità differenti da quelle prescritte dal pubblico potere. Si tratta di un ribaltamento di prospettiva in cui evidentemente il ruolo dello Stato, e la sua eventuale responsabilità, andrebbe fondata non già sulle menzionate regole di attribuzione, ma su una diversa norma primaria riconducibile all'alveo della *due diligence*[40]. Ciò ha evidentemente a che vedere anche con il ricorso

[39] Casi di questo tipo si verificano soprattutto quando organi dello Stato affidino attività specifica a privati che agiscono quali ausiliari dell'organo. In tema si veda FOCARELLI, *Trattato di diritto internazionale*, Milano, 2015, p. 1937.

[40] Lo stessa impostazione potrebbe valere anche nel caso in cui si riscontrasse che il soggetto privato ha agito *ultra vires* rispetto al mandato statale. La difficoltà di uno sviluppo simile è comunque evidente e va vista in parallelo rispetto alla prospettiva di sviluppare un criterio di controllo virtuale come paradigma di superamento della logica del controllo effettivo: come è noto infatti la *Rule* 6 del Tallin Manual, prevede che «*a State bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation*», fa espresso riferimento all'art. 8 del Progetto di Articoli, così confermando la rile-

alla categoria delle obbligazioni positive di tutela dei diritti fondamentali e sul punto si potrà tornare dopo aver dedicato una breve trattazione all'elemento oggettivo dell'illecito.

4. *La ricostruzione dell'elemento oggettivo dell'illecito: il ruolo del diritto consuetudinario e delle norme convenzionali*

L'esame dell'elemento oggettivo, ossia l'antigiuridicità, intesa come contrarietà a precetti di diritto internazionale che si siano consolidati con i tratti della piena giuridicità e vincolatività, deve riguardare in modo distinto il piano del diritto internazionale generale e quello del diritto internazionale convenzionale.

Nel diritto internazionale generale, l'aggancio normativo più diretto è quello con la norma che impone la tutela del dominio riservato e, con esso, della sovranità statale. Si tratta di una dimensione, quella della non ingerenza, che il diritto internazionale classicamente declina in chiave territoriale e questo si collega profondamente con la distinzione, che si è prima introdotta, fra dimensione territoriale o extraterritoriale della condotta[41]. Da questo primo punto di vista, appare arduo ricostruire come contrario a precetti di diritto in-

vanza del criterio del controllo effettivo anche nel contesto del cyberspazio. A ciò si aggiunga che la *Rule* 8 si premura di escludere ogni sussistenza di presunzioni in materia, disponendo che «*the fact that a cyber operation has been routed via the cyber infrastructure located in a State is not sufficient evidence for attributing the operation to that State*».

Giova peraltro ricordare come il punto sia controverso e come, secondo una parte della dottrina, alla parte che invoca la responsabilità di un altro stato per violazione della propria sfera di sovranità sarebbe sufficiente dimostrare che la struttura informatica attraverso la quale la violazione si è realizzata si trovava sul territorio di quello Stato. Tale ricostruzione resterebbe comunque circoscritta ai soli illeciti derivanti dalla violazione di generali obblighi di prevenzione, e postula quindi la ricostruzione di una diversa norma primaria di responsabilità. Sul tema si veda HEINTSCHEL VON HEINEGG, *Legal implications of territorial sovereignty in cyberspace*, in ZOSSECK, OTTIS, ZIOLKOWSKI (eds.), *4th International Conference on Cyber Conflict*, 2012, pp. 17-18.

[41] Sul tema della integrità del cyberspazio si è sviluppato un ampio dibattito (si rinvia in particolare ai *blog EJIL Talk* e *Opinio Juris*), in particolare in relazione al caso NSA, esploso in seguito alle rivelazioni di Edward Snowden . Si veda in tema, fra i molti, PETERS, *Surveillance? The Unlawfulness of the NSA-Panopticon, Parts I and II* in http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-i/ e http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/ (visitati da ultimo il 10 ottobre 2016); si veda altresì WRANGE, *Intervention in National and Private Cyber Space and International Law,* in *The Fourth Biennial Conference of the Asian Society of International Law* (Delhi, 14-16 November 2013) disponibile su http://www.diva-portal.org.

ternazionale generale condotte che non presentino chiare caratteristiche di extraterritorialità. Il che rende delicato soprattutto ricostruire in termini generali l'antigiuridicità di quella che si è definita come 'intercettazione transnazionale'[42] e che è fattispecie quantitativamente assai rilevante del più ampio fenomeno della sorveglianza.

Un altro punto rilevante nella prospettiva del diritto internazionale generale è la necessaria presenza dell'elemento della coercizione che, come evidenziato a più riprese dalla Corte internazionale di giustizia, è funzionale alla configurazione dell'ingerenza come illecita[43]. Alla stregua di quanto si osservava, e impregiudicata la frequente sovrapposizione fra intenti di accesso e di intercettazione abusiva e intenti distruttivi, che già si menzionava in relazione a episodi rilevanti della prassi, occorre evidentemente distinguere i due aspetti per ritrovare l'elemento della coercizione già nei primi. Questo in forza di una interpretazione lata del dovere di non ingerenza che faccia ritenere sussistenti elementi di coercizione, non altrimenti facilmente dimostrabili, tutte le volte che l'accesso o l'intercettazione possano dirsi abusivi in quanto semplicemente non autorizzati[44].

In definitiva, dal punto di vista del diritto internazionale generale e del principio di non ingerenza, il riscontro dell'antigiuridicità sembra senz'altro

[42] Da un lato si richiederebbe infatti il consolidamento nel tempo di una prassi consistente per l'emersione di una norma di segno differente, in cui l'extraterritorialità non sia valutata come elemento intrinseco della condotta, ma invece e più latamente come caratteristica degli effetti che la condotta produce. D'altro canto non mancano visioni del tutto opposte, secondo le quali, muovendo dalla imprescindibilità per così dire 'di sistema' della ricerca dati transfrontaliera, anche e soprattutto in relazione alla repressione del *cybercrime*, si argomenta in difesa della piena legittimità di misure unilaterali di *enforcement* anche extraterritoriale. In tema si veda GOLDSMITH, *The Internet and the Legitimacy of Remote Cross-Border Searches*, in *University of Chicago Public Law and Legal Theory Working Papers*, 2001, p. 13.

[43] Corte internazionale di giustizia, *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States)*, in *I.C.J. Reports 1986*, p. 14, par. 205, in cui la Corte afferma che «*a prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy*».

[44] Sul punto si veda GILL, *Non-intervention in the cyber context*, in ZIOLKOWSKI (ed.), *Peace time regime for State activities in cyber space*, NATO CCD COE, 2013, p. 232 ss. Indicazioni in questo senso sembrano provenire anche dal caso *Timor Leste v. Australia* in cui la CIG ha osservato che l'intercettazione di comunicazioni "personali" dello Stato (in questo caso con i propri legali) e la sottrazione di dati ad esso appartenenti possono costituire un illecito per contrasto con l'art. 2 par. 1 della Carta delle NU, che tutela l'eguaglianza tra gli Stati. Si veda Corte internazionale di giustizia, *Questions relating to the seizure and detention of certain documents and data (Timor-Leste v. Australia), Provisional Measures*, ordinanza del 3 marzo 2014, in *I.C.J. Reports 2014*, p. 147, parr. 22-30.

possibile se l'aspetto abusivo dell'accesso e della intercettazione si collega ad una condotta intrinsecamente extraterritoriale, mentre è più difficile se esso si colleghi a una condotta che pur avendo effetti extraterritoriali, risulta formalmente tenuta sul territorio dello stato. Il che conduce alla difficoltà nel ritenere, da questo punto di vista, l'illiceità sia della fattispecie dell'accesso o intercettazione infra territoriale sia quello della intercettazione cd. transnazionale.

Occorre ora valutare se si possa pervenire a risultati differenti, in punto antigiuridicità, alla luce delle prospettive offerte da strumenti di diritto internazionale convenzionale. Essi, pur dotati di un minore respiro rispetto al generale principio di non ingerenza, sembrano offrire qualche maggiore possibilità di ricostruire la sussistenza dell'antigiuridicità in relazione a condotte non pienamente extraterritoriali: ciò è logico ed evidente se si considera la maggiore specificità dei precetti, che sono volti alla protezione di beni giuridici meglio individuati e circoscritti in una dimensione che può, a certe condizioni, anche prescindere da una autentica extraterritorialità.

Esemplare è in tal senso la tutela del personale diplomatico e la possibilità che semplici attività di sorveglianza, svolte dallo Stato anche in dimensione squisitamente territoriale, come è ben possibile per quanto si affermava rispetto alle opzioni di intercettazione della comunicazione in transito sul proprio territorio, risultino internazionalmente illecite perché aventi ad oggetto o comunque coinvolgenti personale diplomatico, protetto ai sensi della Convenzione di Vienna del 1961 sulle relazioni diplomatiche[45].

L'antigiuridicità può anche discendere da rapporti convenzionali specifici fra due o più Stati, o dal fatto che essi siano parte di una stessa organizzazione internazionale che pone vincoli particolari di cooperazione, trasparenza e lealtà in relazione ai fini statutari. Il caso più evidente in merito riguarda proprio il rapporto fra Stati europei e Stati Uniti in relazione alla *membership* nella NATO.

Più in generale, si può ritenere che in presenza di un vincolo convenzionale che fonda le relazioni amichevoli fra due o più Stati, sia lo stesso principio di buona fede, che attiene alla interpretazione e alla esecuzione dei trattati, a imporre l'astensione da comportamenti di sorveglianza. Questo è particolarmente vero se la sorveglianza si traduce in condotte che siano suscettibili di pregiudicare l'oggetto o lo scopo del trattato, ma si può anche ritenere che la

[45] La prassi mostra come da tempo la Comunità internazionale ritenga inviolabili i documenti e la corrispondenza diplomatica. Cfr. Anche l'art. IV della Convenzione del 1946 sui privilegi e le immunità delle Nazioni Unite, che tutela la «*inviolability of all papers and documents*» degli Stati membri che partecipino ai lavori dell'organizzazione.

buona fede possa, in certi casi e a certe condizioni, far sorgere degli obblighi integrativi di astensione[46].

Altre fonti convenzionali rilevanti in merito sono la Convenzione n. 108 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati, ma anche gli accordi posti sotto l'egida del WTO[47], e in particolare l'accordo TRIPS, in relazione alla antigiuridicità dello spionaggio industriale[48]. Deve poi essere citata l'iniziativa per completare la struttura della Convenzione di Budapest del 2001 sul *Cybercrime* con un Protocollo dedicato espressamente alla sorveglianza e ai suoi limiti, nonché varie fonti speciali relative ai dati dei passeggeri aerei e ai dati finanziari, che possono configurare violazioni di attività di sorveglianza allorché esse travalichino i limiti previsti in relazione ad un efficace contrasto al fenomeno terroristico[49].

Si tratta in definitiva di un panorama assai vario e variegato, che stenta però a comporre un quadro coerente su cui fondare l'elemento della antigiuridi-

[46] Il tema si lega alla portata delle pertinenti disposizioni della Convenzione di Vienna del 1969 sul diritto dei trattati, e in particolare gli artt. 26 e 31. Esso si presenta evidentemente complesso e articolato perché investe la attitudine della buona fede a creare obblighi integrativi rispetto al tessuto convenzionale. Sul punto sia consentito rinviare, nel quadro di una lettera vastissima sul principio, a ODDENINO, *Pactasuntservanda e buona fede nell'applicazione dei trattati internazionali*, Torino, 2003, in particolare p.81 e ss., in cui si ritrovano anche utili considerazioni su come, al contrario, sia arduo sostenere che la buona fede possa essere invocata in generale, e al di fuori di un vincolo convenzionale, come fonte di simili obblighi.

[47] PENG, *Cybersecurity threats and the WTO national security exceptions*, in *Journal of International Economic Law*, 2015, p. 449 ss.

[48] EFFRON, *Secrets and spies: extraterritorial application of the economic espionage act and the trips agreement*, in *New York University Law Review*, 2003, pp. 1481-1484. Il tema dello spionaggio economico è assai rilevante, e non può essere approfondito in questa sede. Per un inquadramento rispetto alle categorie del diritto internazionale si veda PARAJON SKINNER, *An International Law Response to Economic Cyber Espionage,* in *Connecticut Law Review*, 2014, 1165

Per gli obblighi che potrebbero invece discendere da accordi bilaterali di investimento si veda SHACKELFORD, RICHARDS, RAYMOND, CRAIG, *Using BITs to protect bytes: promoting cyber peace by safeguarding trade secrets through bilateral investment treaties*, in *American Business Law Journal*, 2015, p. 52 ss.

Si segnala come anche nell'ordinamento dell'Unione europea la questione sia stata recentemente disciplinata con la Direttiva (UE) 2015/2392 del 17 dicembre 2015, relativa al cd. *whistleblowing*, il cui campo di applicazione si estende necessariamente alle società statali. Sul punto si veda ABAZI, *Tradesecrets and whistleblower protection in the European Union,* in *EuropeanPapers*, 3 ottobre 2016, disponibile su www.europeanpapers.eu.

[49] Si veda la ricostruzione offerta da TERRASI, *Trasmissione dei dati personali e tutela della riservatezza: l'Accordo tra Unione europea e Stati Uniti del 2007*, in *Rivista di diritto internazionale*, 2008, p. 375 ss. Si vedano altresì sul punto le recenti Conclusioni dell'Avvocato generale nella causa A-1/15, presentate l'8 settembre 2016, relative all'accordo tra Unione europea e Canada in materia di trasferimento di *passenger name records*.

cità. In effetti, come nota la dottrina più avveduta, è proprio l'assenza di un quadro condiviso di *standards* di sorveglianza a rendere frequente e inevitabile l'invocazione unilaterale, ad opera dei singoli Stati, tanto, da un lato, delle prerogative discendenti dal principio di non ingerenza offerto dal diritto internazionale generale, quanto, dall'altro, della eccezione della sicurezza nazionale.

5. Segue: *l'elemento oggettivo oltre la dimensione strettamente interstatuale: la prospettiva di tutela dei diritti umani in relazione alla sorveglianza di massa*

Il quadro descritto è focalizzato su una dimensione eminentemente interstatuale del fenomeno: esso è pertanto limitato e deve essere ora calato in una prospettiva più ampia, da porsi in relazione con il dirompente fenomeno della sorveglianza di massa.

Tale più ampia prospettiva appare davvero imprescindibile e fa riferimento ad una dimensione normativa non meno rilevante di quella della tutela della sovranità territoriale, nella forma del principio di non ingerenza, e di quella discendente da vincoli convenzionali che gli Stati tendono a concepire, nella loro portata bi o multilaterale, come pienamente disponibili. È la dimensione per così dire 'verticale' della di tutela dei diritti umani, che muove da evidenti esigenze di assicurare protezione della dignità, della riservatezza e della sfera individuale di ciascuno.

È infatti evidente che la ricostruzione in chiave solo interstatuale, nella sua orizzontalità, è, dal punto di vista della tutela dei diritti individuali, profondamente imperfetta: essa non solo postula la prova di una dimensione extraterritoriale spesso sfuggente, o comunque spesso contestata o controvertibile, ma è altresì soggetta a forti limiti perché la condotta di sorveglianza che concretizza la violazione può spesso avvenire sotto l'egida della scriminante del consenso dello Stato leso[50], o comunque si svolge a fronte di una certa reciproca acquiescenza da parte degli Stati.

La riemersione, a questo proposito, della tutela dei diritti in dimensione individuale è tesa a sottrarre la materia alla sua libera disponibilità ad opera

[50] Certamente si può sostenere che a fronte di attività di sorveglianza massiva la logica del consenso preventivo non possa legittimamente essere invocata, dal momento che esso non potrebbe essere contenuto nei limiti precisi che pure gli sono normativamente prescritti, risultando sostanzialmente un consenso 'in bianco' e, di per ciò stesso, privo di limiti e di oggetto, e dunque incapace di fungere da scriminante. Il punto non fa però venire meno la necessità di dare una diversa impostazione al profilo dell'antigiuridicità, che sia più rispettosa delle istanze individuali.

degli Stati nei rapporti reciproci[51]: si tratta di un richiamo alla tutela dei diritti umani come argine e correttivo dei disequilibri generati dal realismo politico che impregna di sé le relazioni bi o multilaterali, nonché dal mantenimento di uno *status quo* tecnocratico poco bilanciato e ancor meno attento alla dimensione individuale dei diritti[52].

I riferimenti normativi per questa protezione sono evidentemente l'art. 17 del Patto delle Nazioni Unite sui Diritti civili e politici, che ricalca quasi totalmente l'art. 12 della Dichiarazione Universale dei diritti dell'Uomo[53].

Tali fonti sono oggi interpretate e interpretabili con una specifica attenzione per il fenomeno della sorveglianza di massa. In proposito si deve menzionare la recente Risoluzione dell'Assemblea generale delle NU che precisamente offre una simile prospettiva collegando direttamente sorveglianza di massa, condotta anche extraterritorialmente, e art. 12 della Dichiarazione Universale nonché art. 17 del Patto delle Nazioni Unite sui Diritti civili e politici[54].

Si tratta di strumenti direttamente applicabili agli Stati che li hanno ratificati. Tali norme, anche a tacere di una loro possibile caratura consuetudinaria che potrebbe consolidarsi nel tempo, offrono oggi strumenti di tutela efficaci anche in relazione a condotte extraterritoriali. Come infatti ha notato la dottrina più avveduta, l'appellarsi alla extraterritorialità per escludere

[51] Come ben espresso in MILANOVIC, *Human rights treaties and Foreign Surveillance cit.* p. 86, l'importanza di un approccio di tutela dei diritti umani sta nel focalizzarsi «*on the rights and interests of the affected individuals rather than solely on the interests and sovereignty of states*».

[52] In tema di *Privacy* e *Data Protection*, e in relazione alle sempre crescenti e mutevoli esigenze di tutela individuale discendenti dallo sviluppo delle tecnologie informatiche, la letteratura è sterminata. Per un necessario approccio internazionalistico si veda FOCARELLI, *La Privacy. Proteggere idati personali oggi*, Bologna, 2015.

[53] In particolare, l'articolo 17 del Patto recita: «*No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of law against such interference or attacks*». Sul piano regionale, dal quale occorre necessariamente prescindere nell'economia del presente lavoro, il riferimento va all'art. 8 della Convenzione europea dei diritti dell'uomo.

[54] *Resolution on the Right to Privacy in the Digital Age*, G.A. Res 68/167, U.N. Doc. A/RES/68/167 del 17 gennaio 2014, nel cui Preambolo si fa preciso riferimento a una profonda preoccupazione relativamente al «*negative impact that surveillance and/or interception of communications including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and the enjoyment of human rights*». Sul punto extraterritorialità si veda anche il Paragrafo 5 della Risoluzione, mentre in relazione all'obbligo positivo di proteggere è rilevante il riferimento che il Paragrafo 6 fa al dovere degli stati di regolare adeguatamente, in relazione alla tutela della *privacy*, il comportamento di soggetti non statali quali, in particolare, le compagnie di telecomunicazione.

l'applicabilità di tali strumenti è discutibile perché storicamente anacronistico in relazione al profilo tecnologico e logicamente infondato, in relazione al dovere degli Stati di rispettare i diritti in relazione a proprie condotte indipendentemente dal contesto territoriale di riferimento[55].

Parimenti importante è la possibilità di ricostruire, a partire da tali precetti, obblighi positivi di protezione che lo Stato deve assolvere, sul proprio territorio, anche in relazione a comportamenti potenzialmente lesivi tenuti da soggetti privati ad esso estranei, che pare una prospettiva sempre meno fantasiosa nel quadro della sorveglianza di massa e del fenomeno *Big Data*.

6. *Conclusione*

Le considerazioni che precedono confermano appieno che, in tema di violazione di sistemi informatici contenenti informazioni riservate, l'approccio internazionalistico di stampo interstatuale è utile punto di partenza. Un primo ed essenziale tassello per tentare di riportare nell'alveo del diritto, e del diritto internazionale in particolare, prassi diffusissime nel mondo contemporaneo.

L'analisi ha rivelato a questo proposito, e pur nelle difficoltà legate ad una compiuta precisazione degli elementi costitutivi della fattispecie, una possibilità di riscontro abbastanza agevole degli elementi costitutivi dell'illecito, almeno per quanto riguarda condotte extraterritoriali poste in essere direttamente dallo stato o su sua istruzione.

Il punto cruciale che si è evidenziato, peraltro, è che una simile e pur utile ricostruzione non è da sola sufficiente ad affrontare il fenomeno e le sfide, anche normative, poste dalla sorveglianza massiva che si è evocata come fenomeno caratterizzante la nostra epoca. Molte della criticità del tema relativo alla protezione dei dati, anche nella loro dimensione di flusso transfrontaliero, sfuggono oggi ad una efficace descrizione e codificazione nei termini di illecito internazionale interstatuale[56]. Né potrebbe essere altrimenti se si considera

[55] In tema si veda la lucida ricostruzione di MILANOVIC, *Human rights treaties and Foreign Surveillance cit.,* p. 111 e ss. ove, accanto ai classici modelli di applicazione normativa basati sulla logica degli ordinamenti giuridici a base territoriale o personale, si delinea un efficace tertium genus che differenzia la portata territoriale degli obblighi positivi da quella degli obblighi negativi.

[56] Il tema del flusso transfrontaliero dei dati e delle connesse esigenze di tutela è vastissimo e molto dibattuto specie in relazione alla questione del flusso Europa/USA all'indomani della sentenza *Schrems*, già citata, e alla istituzione di un nuovo sistema basato sull'accordo *Privacy Shield*. Esula dall'economia del presente lavoro approfondire tali profili, si fa rinvio, fra i molti riferimenti possibili a RESTA, ZENO ZENCOVICH (a cura di) *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma, 2016.

che il motore del flusso di dati (nella sua manifestazione massiva legate alle capacità computazionali di *Big Data*) è prevalentemente economico ed è saldamente nelle mani di soggetti privati con una spiccata caratterizzazione multinazionale, ma al contempo con un forte radicamento negli Stati Uniti: il potere pubblico di tale Stato, di conseguenza, può per loro tramite irradiarsi senza assumere forme evidenti di azione extraterritoriale.

È su questa circostanza, che determina un vero e proprio cambio di paradigma rispetto alla visione orizzontale e, per così dire, westfaliana dei rapporti interstatuali, che si evidenzia, imprescindibile, la necessità di valorizzare al massimo grado una dimensione di tutela individuale, volta a completare le prospettive dischiuse dall'illecito interstatuale.

In particolare la possibilità di declinare la portata extraterritoriale dei diritti individuali in una duplice dimensione aggiunge importanti prospettive per arginare il fenomeno: da un lato una dimensione negativa, che comporta il dovere, anche extraterritoriale, dello Stato dall'astenersi da violazioni ingiustificate; dall'altro, una dimensione positiva che porta a forme di garanzia dei diritti umani sul territorio dello Stato, anche rispetto a soggetti privati terzi che non sono come tali diretti destinatari di obblighi di tutela dei diritti umani. Si tratta di una prospettiva interessante di parallelismo fra esercizio della sovranità e responsabilità, che è, oggi, da più parti evocata come utile ripensamento del ruolo del diritto internazionale a fronte delle sfide del mondo globalizzato[57].

La necessità di valutare il tema dell'illecito internazionale in questo quadro allargato discende inoltre da un elemento finanche paradossale che si può trarre dall'analisi appena svolta: esiste infatti una relazione precisa e proporzionale fra la portata dei requisiti perché un illecito possa essere attribuito allo stato e il grado di incidenza, in termini di controllo effettivo, che esso deve saper esercitare sul cyberspazio. Ciò porta alla conseguenza paradossale che il postulato di tale attribuzione divengono precisamente delle importanti compressioni del diritto individuale alla *privacy* inteso in senso individuale. Questa è la prova inconfutabile che i due approcci non possono che essere visti come complementari e che il troppo insistere per valorizzare l'uno può risolversi in detrimento per l'altro.

Su un piano ancora differente, che esula peraltro dai confini del presente lavoro, ci si può infine interrogare se, a fronte di una ingente difficoltà nell'affermare a livello internazionale *standards* condivisi di sorveglianza che sappiano tradurre in norme giuridiche efficaci i confini cui sottoporre i comportamenti tecnici, non debba giocoforza farsi strada, a completare il quadro

[57] Sul punto sia consentito rinviare all'approfondimento svolto in ODDENINO, *Law and Territory Happily everAfter: Some Reflection*s on Globalization and Inter*national Law*.

che si è descritto, una terza prospettiva di tutela, connotata in senso ancor prima tecnologico che normativo.

Lo sfondo più ampio su cui la partita della riservatezza si innesta è infatti, giova ricordarlo, quello del sorgere di una sorta di moderno Leviatano della sorveglianza di massa, che opera in virtù di una profonda e per certi versi perversa saldatura del potere pubblico con quello privato, che in una perseguita ambiguità rispetto al loro ruolo, rinunciano a svolgere il ruolo di argine reciproco[58].

Di esso i cittadini sono preda perché proni ad accettare, in cambio dei servizi disponibili nel mondo *online*, di divenire essi stessi, attraverso i propri dati e metadati, merce di scambio. Ciò fa pensare che la protezione debba in qualche misura proporsi di ripartire dalla stessa dimensione tecnologica dell'utilizzo, che va orientata verso forme di uso maggiormente consapevole, di anonimizzazione dei dati e di crittografia nelle comunicazioni, oltre che verso forme di *privacy by default* o *privacy by design* che siano incorporate in radice nei dispositivi tecnologici[59].

Peraltro, quanto ciò possa proteggere la fondamentalità dei diritti individuali in gioco anche al di là, talvolta, della stessa volontà dei destinatari, è impossibile dire.

[58] Il che appare particolarmente indicato se si considera, circostanza non del tutto intuitiva, che la sorveglianza è in realtà facilitata da un contesto di debolezza della dimensione pubblicistica della governance della Rete, ove si realizza una vera supplenza ad opera della dimensione privatistica, tradottasi in che efficacemente è stata definita la '*Internet governance by contract*' In tema il riferimento d'obbligo va a BYGRAVE, *Internet Governance by Contract*, Oxford, 2015. Per quanto in questa sede interessa occorre vedere la tutela dei diritti individuali in Rete come espressione della necessità di arginare, con l'affermazione di valori pubblicistici, l'occupazione dello spazio virtuale ad opera di vincoli contrattuali e *terms of reference* sempre più sofisticati, e finalizzati a salvaguardare il dogma formale del consenso svuotandolo della sua sostanza. Corollario di questa ricostruzione è che l'esigenza di protezione della sfera individuale risulta in Internet tanto acuta in relazione a soggetti che sono espressione del pubblico potere quanto lo è in relazione a soggetti privati, che sono divenuti attori di primo piano capaci di dominare e plasmare la Rete, sviluppandola secondo le linee strategiche del proprio interesse. In relazione a questo delicato punto, con riferimento specifico alle iniziative per una codificazione dei diritti in Rete, si veda, fra i molti riferimenti possibili, NATOLI, *La Dichiarazione dei diritti in internet italiana: una prospettiva internazionalista*, Post su SIDI Blog del 24 settembre 2015, con risposta di ODDENINO, *Code is still Law: la codificazione dei diritti in internet, la tutela dei dati personali e l'arduo contrappunto del diritto alla tecnocrazia*, Post su SIDI Blog del 12 ottobre 2015. In tema si veda altresì CARTA, *Diritto alla vita privata ed Internet nell'esperienza giuridica europea ed internazionale*, in *Il diritto dell'informazione e dell'informatica* 2014, p. 1 ss.

[59] In tema si veda PAGALLO, *Privacy e design*, in *Informatica e diritto*, 2009, p. 123 ss.; PRINCIPATO, *Verso nuovi approcci alla tutela della privacy:* privacy by design *e* privacy by defaults settings, in *Contratto e impresa Europa*, 2015, p. 197 ss.

ABSTRACT

The reconstruction of the violation of information system resources and data as an internationally wrongful act is contended by two poles of attraction: the horizontal dimension of inter-state responsibility and the vertical protection of human rights, particularly in its extraterritorial reach. The investigation of the constitutive elements of responsibility, namely imputability and wrongfulness, reveals some difficulties deriving not only from some definitory shortcomings but also from the awkward application of traditional categories to face some major challenges triggered by the contemporary trends of mass surveillance programs. As a consequence, these issues seem better addressed moving from a more comprehensive viewpoint, encompassing not only the necessary complementarity of the two mentioned dimensions, that deserve to be treated as non-mutually exclusive, but also new frontiers of protection, more oriented towards privacy enhancing technologies such as privacy by design or by default, encryption and anonymizing services.