LUISS GUIDO CARLI

LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

DIPARTIMENTO DI GIURISPRUDENZA

A.A. 2013/2014

TESI IN DIRITTO INTERNAZIONALE

TITOLO: ATTIVITÀ D'INTELLIGENCE E DIRITTO INTERNAZIONALE

CANDIDATO: Riccardo Ridolfi

MATRICOLA: 100503

RELATORE: Prof. Natalino Ronzitti

CORRELATORE: Prof. Carlo Focarelli

INDICE

PREMESSSE

1. **Definizioni e ambito di indagine**
2. **Fonti**
3. **Piano di lavoro**

CAPITOLO I: *INTELLIGENCE* IN TEMPO DI PACE NEL DIRITTO INERNAZIONALE

1. **Questioni giuridiche relative a *intelligence gathering* e spionaggio in tempo di pace**
   - **3.1. Liceità dell'attività di *intelligence* sul piano internazionale**
   - **3.2. Liceità dello spionaggio sul piano internazionale**
   - **3.3. Soluzioni proposte**
4. **Operazioni condotte in luoghi non soggetti a sovranità**
   - **4.1. SIGINT in alto mare: l'incidente della *U.S.S. Pueblo***
   - **4.2. Ricognizione aerea: l'incidente dello U-2**
5. **Spionaggio da parte di agenti diplomatici**
   - **5.1. Il caso Kostadinov**
   - **5.2. L'affare Zakharov - Daniloff**
6. **Violazione di sedi diplomatiche**
7. **Sviluppi recenti nel diritto internazionale: *bulk data collection***
   - **7.1. Provvedimenti in seno all'ONU**
   - ***7.2. Privacy* e dati personali in Europa**
8. **Lo spionaggio economico**
9. **Attività di *intelligence* e libertà d'espressione**
   - **9.1. L'Espionage Act e Wikileaks**
   - **9.2. Spie, *leakers, whistleblowers*: le tutele applicabili**
   - **9.3. Considerazioni**
   - **9.4. Esperienze a confronto: il Consiglio d'Europa**
10. **Il dualismo nella pratica degli Stati**
    - **10.1. Giurisdizione extraterritoriale e *protective principle***

10.2. Genesi del protective principle

10.3. Continua: United States v. Zehe

CAPITOLO II – L'UNIONE EUROPEA E GLI STATI UNITI: SCONTRO FRA CULTURE IN MATERIA DI *PRIVACY* E DATI PERSONALI

1. Introduzione

2. Il quadro normativo

2.1. Convenzioni internazionali e *soft law*

2.1.1. La Dichiarazione Universale dei Diritti dell'Uomo

2.1.2. Il Patto internazionale sui Diritti Civili e Politici

2.1.3. Risoluzione dell'Assemblea Generale: *The Right to Privacy in the Digital Age*

2.2. La normativa UE e CEDU

2.2.1. Il Concetto di *Habeas Data* in Europa

2.2.2. Il Consiglio d'Europa: Art. 8 CEDU, Convenzione 108 e nuove proposte normative

2.2.3. La Direttiva 95/46/CE

2.2.4. Continua: l'efficacia transnazionale del RGPD

2.3. Trasferimenti di dati tra USA e UE: l'accordo *Safe Harbor*

2.4. La normativa USA

2.4.1. Evoluzione giurisprudenziale del IV emendamento

2.4.2. La *privacy* negli USA dopo *Katz*: *Wiretap Statute*, FISA e USA PATRIOT Act

2.4.3. Il FISA *Amendments Act* 2008 e la Corte FISA

3. Soluzioni proposte

3.1. La negoziazione dello *Umbrella Agreement*

3.2. La ACLU: proposta di revisione per il *General Comment* 16

3.3. La teoria della *quantitative privacy*

CAPITOLO III: ATTIVITÀ DI *INTELLIGENCE* IN TEMPO DI GUERRA

1. *Intelligence* tra parti belligeranti

2. Spionaggio in tempo di guerra

2.1. Le prime codificazioni

2.2. Le Convenzioni di Ginevra del 1949 ed il I Protocollo Addizionale

2.2.1. Lo status di prigioniero di guerra

2.2.2. Spie nei territori occupati

2.3. La consuetudine ed i manuali militari

2.4. Il trattamento della spia – Considerazioni

CAPITOLO IV: L'*INTELLIGENCE* IN ITALIA

1. L'Italia dopo *Datagate* - Il Garante della Privacy

1.1. Il recepimento della Direttiva 95/46/CE in Italia

1.2. Continua – Il Garante della Privacy

2. Agenzie di *intelligence* italiane - AISE e AISI

2.1. La legge 124/2007 ed il SIS

2.2. Il segreto di Stato

2.3. Considerazioni

CONCLUSIONI

PREMESSE

1. Definizioni e ambito di indagine

Il termine *intelligence* deriva dal latino *intus legere*, "leggere dentro".[1] In questo senso, l'*intelligence* è mera ricerca della conoscenza.[2] Già nella sua traduzione letterale, tuttavia, il termine rivela un *quid pluris*. Si tratta del principale dei suoi elementi costitutivi, necessario ma non sufficiente: la clandestinità. Ai fini della presente ricerca, il campo verrà ristretto all'attività di *intelligence* quando strumentale al processo decisionale politico: "*[i]ntelligence differs from mere information because of its value against a specific decisional goal.*"[3] Se ne deduce che l'attività di *intelligence gathering*[4] è posta in essere dai governi nazionali al fine di ottenere informazioni in segreto, vale a dire senza il consenso dello Stato che controlla dette informazioni.[5] Giova specificare, a questo punto, che le parole *intelligence* e spionaggio non sono sinonimi.[6] *Intelligence* vuole essere un termine onnicomprensivo, *genus* che racchiude diverse altre *species*. L'*intelligence* indirizzata verso fonti informative umane (in dottrina nota come HUMINT) tra queste è la più ampia e ricomprende, senza limitarsi ad esso,

[1] CARACCIOLO L., *Homo curiosus* in 7 Limes Rivista Italiana di Geopolitica, 2014, 7.
[2] G B DEMAREST, "Espionage in International Law" (1995-1996) 24 Denv J Int'l L & Pol'y 322.
[3] *G* B DEMAREST, *op. cit.* 323.
[4] Nella letteratura ricorre spesso anche la dicitura *intelligence collection*.
[5] S CHESTERMAN, "Secret Intelligence" (2009) Max Planck Encyclopedia of Public International Law, Oxford University Press: http://opil.ouplaw.com/home/EPIL; vd. anche A J RADSAN, "The Unresolved Equation of Espionage and International Law" (2006-2007) 28 Mich J Int'l L 600; Executive Order 12333 (1982) 3 §3.4(d) : "Foreign intelligence *means information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities*"; Central Intelligence Agency Office of Personnel, Central Intelligence Agency 3 (1993): "*Intelligence is information: information about adversaries and potential adversaries that nations gather to formulate their foreign and security policies.*"; Central Intelligence Office of Personnel, Central Intelligence Agency 2 (1976): "*In international affairs Intelligence is knowledge-fact and estimate [...] The London Economist defined intelligence this way: «Modern intelligence has to do with the painstaking collection and analysis of fact, the exercise of judgment, and clear and quick presentation. It is not simply what serious journalists would always produce if they had time; it is something more rigorous, continuous, and above all operational […] that is to say, related to something that somebody wants to do or may be forced to do.*»; J SIMS, *U.S Intelligence at the Crossroads: Agendas for Reform* (Roy Godson & al edn, 1995) 4: "*Intelligence is best defined as information collected, organized or analyzed on behalf of actors or decision makers.*"; G B DEMAREST, *op.cit.* 322-323.
[6] A J RADSAN, "The Unresolved Equation of Espionage and International Law" (2006-2007) 28 Mich J Int'l L 599; cfr. G B DEMAREST, *op. cit.*; C FORCESE, "Spies Without Borders: International Law and Intelligence Collection" (2011-2012) 5 J Nat'l Sec L & Pol'y 181.

lo spionaggio.[7] Esempi di HUMINT diversa dallo spionaggio possono essere la raccolta di informazioni ottenute da rifugiati, articoli redatti dalla stampa, interviste, osservazioni del personale diplomatico all'estero.[8] L'*intelligence* delle comunicazioni e degli strumenti elettronici (c.d. SIGINT o *Signals Intelligence*),[9] ricomprende le intercettazioni dei mezzi di comunicazione ed altre forme di *intelligence* elettronica.[10] In tempi relativamente recenti, seguendo lo sviluppo tecnologico, sono nate nuove sottocategorie quali la MASINT (*Measurement and Signature Intelligence*), IMINT (*Photo or Imagery Intelligence*),[11] nonché diverse altre "-INT" [12] che a poco serve elencare in questa sede. Nell'era della digitalizzazione non è azzardato sostenere che possono essere tutte ricondotte all'*intelligence* dei segnali elettronici. [13] Parimenti non si può ignorare l'osservazione, qui condivisa, secondo la quale: "senza *human factor* le discariche dei dati «oggettivi» affastellati dai rami Imint (immagini), Masint (misure) e Sigint (segnali) resterebbero materia inerte."[14] In definitiva, volendo ricostruire una definizione unitaria di *intelligence*, si può affermare che questa è la raccolta clandestina di informazioni senza il consenso dello Stato *target*, operata con qualsiasi mezzo, strumentale al processo decisionale politico dello Stato mandante.

Quale che sia la forma assunta dall'attività d'*intelligence*, ciò che rileva evidenziare è come questa sia il prodotto del lavoro di agenzie segrete incaricate dai rispettivi governi. Generalmente il compito loro attribuito è quello di valutare rischi e circostanze in un dato momento storico per guidare le azioni strategiche, militari, politiche.[15] Ciò detto, non si deve credere che la raccolta di informazioni esaurisca le mansioni degli organi preposti all'*intelligence gathering*. Prendendo ad esempio la CIA statunitense (*Central Intelligence Agency*),[16] si nota una ripartizione in due principali sezioni: il *Directorate of Operation* ed il *Directorate*

[7] G B DEMAREST, *op. cit.* 324; C FORCESE, *op. cit.* 182-183.
[8] *Ibidem*.
[9] S CHESTERMAN, *op. cit.*; *G* B DEMAREST, "Espionage in International Law" (1995-1996) 24 Denv J Int'l L & Pol'y 324.
[10] S CHESTERMAN, *op. cit.* §1; G B DEMAREST, *op.cit.*
[11] Si pensi ai satelliti di ricognizione quali TecSAR o MIDAS.
[12] S CHESTERMAN, *op. cit.*
[13] *Ibidem*; G B DEMAREST, *op. cit.* 324.
[14] CARACCIOLO L., *op. cit.* 8.
[15] S CHESTERMAN, *op. cit.* §1.
[16] L'esperienza USA nel campo dell'*intelligence* verrà approfondita *infra*.

of Intelligence.[17] Mentre i c.d. *case officers* inquadrati nella prima sezione in parola hanno il compito di raccogliere le informazioni, queste ultime devono poi essere elaborate dai c.d. "analisti" della seconda sezione.[18] Possiamo dunque arricchire la definizione di *intelligence* fornita finora riconoscendo la presenza di due momenti cardinali, vale a dire raccolta e analisi delle informazioni.[19] L'analista si limita a elaborare l'*intelligence* attraverso il metodo scientifico e pertanto non è considerato una spia.[20] La divisione dei ruoli non è casuale. Lo scopo è quello di tenere separato chi ottiene l'informazione "grezza" da chi la analizza, evitando una sovrastima dei dati raccolti nel complesso o da una fonte specifica.[21] Dal punto di vista giuridico sorgono questioni diverse a seconda delle mansioni assegnate all'agente, se non altro perché l'analista non avrà la necessità di introdursi fisicamente nel territorio di un altro Stato sovrano. Sebbene il progresso tecnologico abbia sostanzialmente ridotto la distanza tra analista e agente operativo, bisogna sempre tenere a mente che la presenza di personale sul campo rimane imprescindibile nella maggioranza dei casi.[22]

Le prime forme di spionaggio della storia sono risalenti nel tempo: vi sono testimonianze tanto nella Bibbia,[23] quanto ne "L'arte della Guerra" del filosofo Sun Tsu.[24] Pur a fronte di una storia così ricca, non è semplice ottenere una definizione utile al giurista, posto che si voglia rimanere al di fuori del diritto umanitario.[25] Il DEMAREST[26] ha cercato di ricavare dall'opera dello storico inglese M. BURN[27] una definizione giuridica:

---

[17] J RADSAN, *op. cit.*
[18] *Ibidem.*
[19] S CHESTERMAN, *op. cit.* §2.
[20] G B DEMAREST, *op. cit.* 323; per una definizione di spia vd. *infra*.
[21] S CHESTERMAN, *op. cit.* §2; M HERMAN, *Intelligence Services in the Information Age: Theory and Practice* (Frank Cass London 2001) 111-112.
[22] K JENNINGS, "Espionage: Anything Goes?" (1986-1987) 14 Pepp L Rev 649-650; CARACCIOLO L., *op. cit.*
[23] *Cfr.* GROZIO U., *Le Leggi della Guerra e della Pace III* (Oxford, 1925) 655; G B DEMAREST, *op. cit.* 331.
[24] *Cfr.* A S HULNICK, "Espionage: Does it Have a Future In The 21st Century?" (2004-2005) 11 Brown J World Aff 165.
[25] Vd. *infra*.
[26] G B DEMAREST, *op. cit.* 325-327
[27] M BURN, *The Debatable Land: A study of The Motive of the Spies in Two Ages* (1970) 2: l'autore sintetizza le caratteristiche della spia come segue: "1) *He is deliberately involved in the conveying of information about people or things recently observed*. 2) *He acquires or sends it secretly*. 3) *The information he seeks or conveys is for the use of people hostile to or suspicious of*

> *[E]spionage can be defined as the consciously deceitful collection of information, ordered by a government or organization hostile to or suspicious of those the information concerns, accomplished by humans unauthorized by the target to do the collection.*[28]

L'enunciato è coerente in molti punti con quanto detto finora. Come anticipato *supra*, lo spionaggio è una particolare forma di *intelligence gathering* (attinente alla sola fase di raccolta delle informazioni),[29] che si caratterizza per l'impiego di agenti (come i sopra citati *case officers*) al fine di perseguire l'obiettivo loro assegnato. In relazione a tale definizione, si rendono necessari dei correttivi. Innanzitutto, il DEMAREST non specifica che l'agente[30] debba trovarsi fisicamente nel territorio in cui è situato il *target*. Un simile elemento costitutivo non è privo d'importanza: penetrare ed operare clandestinamente nel territorio di uno Stato estero senza il consenso di quest'ultimo, integra infatti una violazione della sovranità territoriale.[31] Come giustamente è stato osservato,[32] lo spionaggio consistente in forme di sorveglianza elettronica non può essere incluso in questa definizione ristretta. Corrisponde piuttosto ad una forma di SIGINT. Il secondo punto critico è nell'elemento di ostilità (*government or organization hostile*)[33] che l'autore riconosce nei confronti del *target*.[34] Le recenti rivelazioni fatte alla stampa dall'ex-collaboratore della NSA, Edward Snowden, dimostrano (*rectius*

---

those it is about, and it is usually for and about people in government positions, or thought to be threatening to a Government. 4) *He is consciously a deceiver"*; G B DEMAREST, *op. cit. 325.*

[28] G B DEMAREST, *op. cit.* 325-326; per una definizione letterale di spia vd. *Concise Oxford Dictionary of Current English* (1990): "*a person who secretly collects and reports information on the activities, movements, etc of an enemy, competitor* […] *a person who keeps watch on others*".

[29] *Cfr. supra*: lo spionaggio è una forma di HUMINT. *Cfr.* "Senate Select Committee on Intelligence, 99th Congres, 2nd Session, Report on Espionage, Meeting the Espionage Challenge: A Review of United States Counter Intelligence and Security Programs" (Ottobre 1986) 7 Commission Print 28-29: "*The human dimension begins with the trained intelligence officer, dispatched under official or nonofficial cover to operate abroad. […] [I]ntelligence officers recruit and handle agents who are employed by foreign governments, industries, or political organizations"*; K JENNINGS, *op. cit.* 649-650.

[30] *Cfr. supra*: il termine *human* non lascia dubbi in merito al fatto che l'atto di spionaggio *stricto sensu* sia compiuto da esseri umani, senza la mediazione di strumenti di comunicazione, satelliti od i più moderni droni. L'unico mezzo a disposizione della spia è l'inganno (*deceitful collection*).

[31] RONZITTI N., "Il Caso Snowden e le Regole dello Spionaggio" (2013) Affari Internazionali: http://www.affarinternazionali.it/articolo.asp?ID=2369.

[32] C D BAKER, "Tolerance of International Espionage: A Functional Approach" (2003) 19 n°5 Am U Int'l L Rev 1093-1094.

[33] Vd. *supra*.

[34] *Cfr.* G B DEMAREST, *op. cit.* 326.

confermano) l'esistenza di un'ampia pratica di *intelligence gathering* e spionaggio anche nei confronti di paesi alleati.

Il quadro provvisoriamente delineato assume nuove sfaccettature se si considera che lo spionaggio può non limitarsi alla semplice raccolta di informazioni. Si fa riferimento, nello specifico, alle cd. *covert actions* ("operazioni coperte"). Prendendo di nuovo ad esempio il diritto statunitense, l'atto costitutivo della CIA le definisce come: "*activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly.*"[35] Simili attività, per la loro natura, sono state aspramente criticate.[36] Parte della dottrina[37] avrebbe addirittura ravvisato in esse una violazione dell'articolo 2(4) della Carta delle Nazioni Unite, dal momento che le *covert actions*, oltre a costituire un'illecita ingerenza negli affari interni dello Stato straniero, ne metterebbero in pericolo "l'integrità territoriale o l'indipendenza politica".[38] Tuttavia, questa posizione non è accettabile. Per come è stato formulato, l'Art. 2(4) richiede espressamente un'ulteriore condizione: la minaccia o l'uso della forza.[39] In realtà, nella pratica spionaggio e *covert actions* non sono di facile distinzione.[40] Ciò può dirsi specialmente con riferimento alla c.d. "militarizzazione" della CIA, avvenuta a seguito degli attentati dell'11 Settembre 2001 e, con rinnovato vigore, dal 2008 (quando con il beneplacito del

[35] "[A]n activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly": The National Security Act 1947 (2000) 50 U.S.C. § 413b(e); J RADSAN *op. cit.* 599.

[36] G B DEMAREST, *op.cit.* 329; cfr. P AGEE, *Inside the Company: CIA Diary* (1975); D A PHILLIPS, *The Night Watch* (Ballantine Books, 1977); V MARCHETTI & J MARKS, *The CIA and The Cult of Intelligence* (London, Jonathan Cape, 1974); J B SMITH, *Portrait of a Cold Warrior* (Ballantine Books, 1976).

[37] G B DEMAREST, *op. cit.* 330; cfr. A J RADSAN, *op. cit.* 605; *cfr.* Q WRIGHT, *Essays on Espionage and International Law* (Roland Stanger edn, 1962).

[38] Articolo 2(4), Carta delle Nazioni Unite 1945.

[39] La dottrina contestata *supra* fa riferimento in particolar modo allo scandalo *Iran-Contra* che vide protagonisti i servizi segreti USA negli anni '80. Cfr. J PERSICO, *Casey: from the OSS to the CIA* (New York, Viking edn, 1990); N PETERSEN, *American Intelligence: 1775-1990: A Bibliographical Guide* (Claremont, Regina Books edn, 1992); G B DEMAREST, *op. cit.* 330.

[40] *Cfr.* G B DEMAREST, *op. cit.* 330: "*[W]hile covert action can be academically distinguished from human intelligence gathering, the two activities may be blurred in practice. […] Nevertheless, covert action is not espionage, but some espionage activities may constitute covert action.*"

Presidente Obama è stato incrementato esponenzialmente l'impiego dei droni).[41] Spesso le *covert actions* sono compiute senza ricorrere affatto alla forza armata, ad esempio fomentando proteste contro un governo sgradito. In questi casi si rientra ancora nella categoria dello spionaggio. Al contrario, qualora l'agente segreto faccia uso della forza in uno Stato estero, bisognerà fare riferimento alle regole dello *jus ad bellum* per ricercarne una eventuale violazione.

Il caso *Nicaragua v. Stati Uniti,* [42] giudicato di fronte alla Corte Internazionale di Giustizia, mostra una situazione ancora diversa e peculiare. In quella sede, alla Corte fu chiesto di valutare la liceità di atti volti ad armare, addestrare ed offrire supporto logistico ai *contras*.[43] In merito ad essi, non fu possibile dimostrare una dipendenza dei *contras* dal supporto statunitense, tale da poter ravvisare una violazione del divieto dell'uso della forza. D'altro canto, emerse che simili attività di supporto (tra cui figuravano vere e proprie attività di *intelligence*) avevano integrato la violazione di un diverso principio: quello di non ingerenza negli affari interni di uno Stato sovrano.[44]

2. Fonti

Terminata la rassegna dei caratteri basilari del fenomeno *intelligence*, è doveroso premettere a quali fonti normative si attingerà nelle prossime pagine, per inquadrare una realtà così multiforme nel contesto giuridico internazionale e locale. In primo luogo sarà operata una distinzione tra diritto internazionale in tempo di pace e diritto internazionale dei conflitti armati. Il primo presenta le criticità maggiori, per la mancanza di accordi multilaterali o bilaterali dedicati. Piuttosto, si sfrutteranno fonti attinenti ad aree tematiche diverse, cercando di volta in volta la presenza di disposizioni adattabili alla fattispecie della raccolta clandestina di informazioni. Nell'analizzare gli attriti tra attività di spionaggio e sovranità territoriale, il riferimento principale sarà (oltre che alla consuetudine) alla Risoluzione A/RES/25/2625 dell'Assemblea Generale delle Nazioni Unite,

[41] FAINI M., *Lo Spionaggio Industriale Allarga la Faglia del Pacifico* in 7 Limes Rivista Italiana di Geopolitica, 2014, 79.
[42] Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) Merits, Judgment of 27 June 1986, ICJ.
[43] *Ibidem.*
[44] C FORCESE, *op. cit.* 198; D FLECK, *Individual and State Responsibility for Intelligence Gathering* [2007] 28 Mich J Int'l L 687, 691-692.

concernente le relazioni amichevoli e la cooperazione fra gli Stati. Considerando le particolari fattispecie di spionaggio condotte in aree non soggette alla sovranità di alcuno, verranno evocate le disposizioni applicabili in tema di diritto del mare (soprattutto la Convenzione di Ginevra sul mare territoriale e la zona contigua, nonché la UNCLOS) e dello spazio aereo (i.a. il Trattato sui cieli aperti prodotto in seno all'OSCE). In seguito si avrà modo di attestare l'esistenza di una casistica discretamente ricca nell'ambito del diritto diplomatico. Si procederà esaminando alcune situazioni in cui la Convenzione di Vienna sulle relazioni diplomatiche del 1961 è stata sottoposta ad abusi o palesemente violata. Approfondendo alcuni degli aspetti secondari (comunque importanti) legati a *intelligence* e spionaggio, muterà ulteriormente il sistema delle fonti. In tema di spionaggio economico, gli strumenti normativi di rilievo saranno strettamente legati alla tutela della proprietà intellettuale, segnatamente la Convenzione di Parigi per la Protezione della Proprietà Industriale del 1967 e l'accordo TRIPs. Sul piano delle interrelazioni tra *intelligence* e libertà d'espressione, la quantità di riferimenti giuridici si moltiplica. Rimandando all'approfondimento svolto nei relativi paragrafi, si preannuncia uno sdoppiamento tra fonti nazionali (i.a. *Espionage Act* statunitense del 1917, *Executive Order* No. 13526 del 2009, *Whistleblower Protection Act* del 1989 e *Intelligence Community Whistleblower Protection Act* del 1998) e fonti internazionali (Risoluzione del Consiglio d'Europa 1954 del 2013 denominata *National Security and Access to Information*, *Council of Europe Convention on the Access to Official Documents* del 2009, *Global Principles on National Security and the Right to Information* redatti dalla *Open Society Foundations* nel 2013).

Una simile dicotomia caratterizzerà la trattazione di un altro aspetto fondamentale, che discende dall'attività di *intelligence*: il contrasto tra *mass surveillance* operata per ragioni di sicurezza nazionale e diritti umani dei cittadini, in particolare *privacy* e tutela dei dati personali. Dopo aver richiamato le principali fonti internazionali in materia (i.e. la Dichiarazione Universale dei Diritti dell'Uomo, il Patto internazionale sui diritti civili e politici, la recente Risoluzione dell'Assemblea Generale *Right to Privacy in the Digital Age*) seguirà una comparazione tra le fonti europee (Convenzione 108 del Consiglio d'Europa,

CEDU), comunitarie (Direttiva 46/95/CE, proposta di Regolamento generale sulla protezione dei dati)[45] e statunitensi. Data la disarticolazione delle norme sulla *privacy* in America, si guarderà solo agli statuti più incisivi su tale diritto e sul quarto emendamento alla Costituzione degli Stati Uniti, vale a dire lo USA PATRIOT Act 2001, il *Foreign Intelligence Surveillance Act* del 1978 e il relativo FISA *Amendments Act* del 2008. Non saranno ignorati i mezzi di raccordo tra le due realtà occidentali: sarà prestata debita attenzione anche agli accordi bilaterali USA-UE aventi ad oggetto il trasferimento di dati personali: il *Safe Harbor Agreement* e il cd. *Umbrella Agreement* (la cui negoziazione è ancora in corso).

Infine, sarà condotto un raffronto con l'assetto giuridico dato all'*intelligence* in Italia. A tal fine, si studieranno caratteristiche ed effetti dei due pilastri normativi presenti nel nostro ordinamento: il d.lgs. 196/2003 (attuativo della Direttiva 46/95/CE) e la l. 124/2007, che costituisce la fonte unitaria in materia di servizi di informazione per la sicurezza e segreto di Stato.

In merito al diritto internazionale in tempo di guerra, il panorama giuridico è nettamente più ristretto e lineare. La disciplina dello spionaggio (poco o nulla è stato disposto in merito all'*intelligence lato sensu*) è espressamente regolata dai principali strumenti di diritto dei conflitti armati via terra: il *Lieber Code*, la Dichiarazione di Bruxelles (fonti più risalenti, datate rispettivamente 1863 e 1874), le quattro Convenzioni di Ginevra del 1949 ed il primo Protocollo Addizionale del 1977.

3. Piano di lavoro

Guardando alle disposizioni che saranno oggetto di studio, è già possibile intuire la struttura della trattazione che seguirà. Il primo capitolo, dedicato ad *intelligence* e spionaggio in tempo di pace, si focalizzerà quasi unicamente su aspetti di diritto internazionale pubblico. Il nucleo di questa prima parte consta di quattro aree tematiche: le zone non soggette alla sovranità degli Stati, l'abuso delle immunità diplomatiche, la violazione di sedi diplomatiche e la violazione della *privacy* come diritto umano. Essenzialmente si cercherà di dimostrare che

[45] *Rectius*, la proposta di Regolamento non appartiene propriamente al diritto comunitario, bensì dell'Unione Europea.

l'*intelligence gathering* non configura un illecito internazionale per sé solo, ma al momento dell'esecuzione è inevitabile che l'operato degli agenti entri in conflitto con le norme appartenenti agli ambiti su menzionati. La parte finale del capitolo approfondirà degli aspetti di contorno i.e. la liceità dello spionaggio economico, gli standard internazionali di tutela offerti ai cd. *whistleblowers* e gli strumenti processuali utilizzabili contro le presunte spie.

Il secondo capitolo si concentra sulla *bulk data collection* e sulle ripercussioni che le operazioni di sorveglianza massiva e indiscriminata hanno sul diritto alla *privacy* dei cittadini. Si guarderà brevemente agli accordi multilaterali e agli strumenti di *soft law* esistenti per poi procedere con il confronto diretto tra ordinamenti sovranazionali europei e assetto giuridico USA. Si noterà da subito un divario netto per ciò che concerne le garanzie di tutela nei due continenti, con gli Stati Uniti chiaramente sbilanciati a favore della protezione della sicurezza nazionale. D'altro canto, si cercherà di dimostrare che anche in America la Costituzione e la giurisprudenza più progressista hanno un potenziale inestimabile per combattere l'arbitrio delle agenzie federali e porre fine, nel prossimo futuro, alla *mass surveillance*.

Il terzo capitolo esplora il ben diverso contesto dei conflitti armati: le norme codificate, la consuetudine, il trattamento della spia catturata dal nemico. La parte finale sarà riservata ad alcune considerazioni in merito alla opportunità (prevista dalle convenzioni in vigore) che l'agente sia "lasciato indietro" dallo Stato nazionale quando anche i suoi diritti fondamentali siano minacciati o violati.

Il quarto e ultimo capitolo guarda alla situazione corrente in Italia. Nel nostro Stato, il Garante *privacy* si è rivelato particolarmente attivo in risposta alla vicenda *datagate* e sarà perciò oggetto di studio. Parimenti, sarà fornito un quadro d'insieme sull'assetto dell'*intelligence* italiana a seguito della riforma del 2007, con un'attenzione speciale rivolta alle delicate questioni costituzionali che discendono dalla connaturale segretezza con la quale operano le nostre Agenzie.

CAPITOLO I: *INTELLIGENCE* IN TEMPO DI PACE NEL DIRITTO INTERNAZIONALE

1. Questioni giuridiche relative a *intelligence gathering* e spionaggio in tempo di pace

Nella dottrina classica è opinione diffusa che tanto l'*intelligence* quanto lo spionaggio in tempo di pace riguardino unicamente il diritto interno.[46] In tutti gli Stati moderni,[47] simili attività sono incluse dai legislatori nel novero di crimini quali tradimento e sedizione.[48] Nel diritto internazionale, si è detto, è complicato riuscire a delineare regole precise dal momento che non esistono trattati che affrontino la materia in modo diretto.[49] Lo scopo della presente trattazione sarà dunque quello di inferire dalla casistica tradizionale norme di diritto consuetudinario, se effettivamente possibile.

1.1. Liceità dell'attività di *intelligence* sul piano internazionale

La prima difficoltà che si incontra quando si tenta di determinare la liceità dell'attività di *intelligence* è nel trovare una definizione comunemente accettata. Spesso la dottrina confonde l'*intelligence* con lo spionaggio, con la SIGINT o con un non meglio specificato concetto di "sorveglianza". Tuttavia, saper classificare è essenziale in una materia come quella in esame, che presenta questioni giuridiche diverse a seconda delle situazioni. Proprio per l'ampiezza del termine, è impossibile pronunciarsi sulla liceità dell'*intelligence gathering* in termini assoluti. La raccolta di informazioni in sé considerata è un'attività neutra, che non si può scollegare dalle modalità d'esecuzione e dal *target* prestabilito. I paragrafi seguenti analizzeranno l'*intelligence* nelle sue varie forme, individuando di volta in volta le problematiche sollevate ed i possibili rimedi giuridici.

1.2. Liceità dello spionaggio sul piano internazionale

[46] G B DEMAREST, *op. cit.*; R A Falk, *Essayson Espionage and International Law, op. cit.,* A J Radsan, *op. cit.*; RONZITTI N., *op. cit.*
[47] N P WARD, "Espionage and the Forfeiture of Diplomatic Immunity" (1977) 11 Int'l L 663.
[48] G B DEMAREST, *op.cit.* 338.
[49] J RADSAN, *op. cit.* 606; RONZITTI N., *op. cit.*

Le parole di L. OPPENHEIM forniscono un valido punto di partenza per individuare le principali questioni legate allo spionaggio in tempo di pace:

> *Although all States constantly or occasionally send spies abroad, and although it is not considered wrong morally, politically, or legally to do so, such spies have, of course, no recognized position whatever according to International Law, since they are not official agents of States for the purpose of international relations. Every State punishes them severely if they are caught committing an act which is a crime by the law of the land.* […] *A spy cannot legally excuse himself by pleading that he only executed the orders of his Government.*[50]

In primo luogo, interessa evidenziare una criticità evidente: la spia non ha una posizione riconosciuta nel diritto internazionale. A fronte della mancanza di una disciplina sistematica, sono state sviluppate soluzioni giuridiche diverse e spesso discordanti.

Nella dottrina tradizionale esistono per l'appunto tre approcci differenti in merito alla liceità o meno dello spionaggio in tempo di pace.[51] Per un primo orientamento lo spionaggio in tempo di pace è lecito.[52] L'orientamento diametralmente opposto afferma che lo spionaggio in tempo di pace è illecito.[53] Un terzo gruppo si colloca nel mezzo, tentando una mediazione tra le due teorie. Questa mancanza di consenso conferma come non sia possibile estrapolare dalla disciplina classica una *opinio juris* uniforme, né dunque norme di diritto consuetudinario comunemente riconosciute.

La dottrina a favore della liceità dello spionaggio in tempo di pace, ammette tale pratica come atto "non amichevole" sul piano delle relazioni internazionali.[54] Il perno dell'argomentazione è nella mancata violazione di norme di diritto internazionale vigenti.[55]

---

[50] L OPPENHEIM, *International Law* (8th edn, H Lauterpacht, 1955) 862; C C MORRISON JR, "International Law and the Seizure of the USS Pueblo" (1968) 4 Tex Int'l L F 192.
[51] A J RADSAN, *op. cit.*
[52] *Ibidem,* 602; M R GARCIA-MORA, "Treason, Sedition and Espionage as Political Offenses Under the Law of Extradition" (1964) 26 U Pitt L Rev 79-80; G B DEMAREST, *op.cit.* 338.
[53] C FORCESE, *op. cit.* 203; I DELUPIS, "Foreign Warships and Immunity for Espionage" (1984) 78 Am J Int'l L 53, 67; M GARCIA-MORA, *op. cit.* 65-79-80.
[54] A J RADSAN, *op. cit.* 603; G B DEMAREST, *op. cit.* 321.
[55] A J RADSAN, *op. cit.* 603; G B Demarest, *op. cit.* 347.

Il pensiero del Comandante R. SCOTT, offre un contributo ulteriore. Egli, pur consapevole dell'ambiguità dello spionaggio nel diritto internazionale in tempo di pace, non lo ritiene una "*fundamentally wrongful activity*".[56] Con questa formulazione, come l'autore stesso chiarisce, si intende che lo spionaggio non viola principi di *jus cogens*.[57] Proseguendo, egli arriva ad asserire che lo spionaggio sarebbe funzionale al diritto alla legittima difesa preventiva, dunque strumentale al mantenimento di pace e sicurezza internazionali.

Anche questo orientamento, che pure sostiene la liceità dello spionaggio, non rinnega la presenza di criticità. Nella pratica internazionale si nota la diffusione di un cd. "doppio standard":[58] la maggioranza degli Stati, pur conducendo operazioni di spionaggio e riconoscendo che queste vengano realizzate nei loro confronti, si riservano il diritto di perseguire coloro che compiono atti di spionaggio nel proprio territorio.[59] Questa pragmatica osservazione risulta avere molto in comune con l'orientamento dottrinale del "terzo gruppo"[60] (cui si rimanda *infra*).

Un secondo orientamento riconosce nell'attività di spionaggio una violazione del diritto internazionale.[61] La ragione sottesa consisterebbe nel riconoscimento dell'obbligo in capo ai vari Stati di rispettare l'integrità territoriale e l'indipendenza politica altrui.[62] Di conseguenza, il fatto stesso di inviare clandestinamente agenti all'estero sarebbe oggetto di condanna.[63] Al fine di rafforzare questa posizione, viene invocata anche la pratica pressoché uniforme dei legislatori nazionali consistente nel prevedere e punire lo spionaggio come reato.[64]

Si noti che neanche la presente dottrina, pur antitetica alla prima, arriva a qualificare lo spionaggio come un crimine internazionale. Non c'è congruenza,

---

[56] R D SCOTT, "Territorially Intrusive Intelligence Collection and International Law" (1999) 46 A F L Rev 217-218; A J RADSAN, *op. cit.* 604.
[57] *Ibidem*.
[58] R D SCOTT, *op. cit.* 226; A J RADSAN, *op. cit.* 604.
[59] *Ibidem*.
[60] *Cfr. infra*.
[61] M R GARCIA-MORA, *op. cit.* 79-80; Q WRIGHT, "Espionage and the Doctrine of Non-Intervention in Internal Affairs" in *Essays on Espionage and International Law*, *op. cit.*; I DELUPIS, "Foreign Warships and Immunity for Espionage" (1984) 78 Am J Int'l L.
[62] Q WRIGHT, *op cit.* 12; A J RADSAN, *op.cit.* 605.
[63] I DELUPIS, *op. cit.* 53, 67; A J RADSAN, *op.cit.* 605.
[64] C D BAKER, *op. cit.* 1097.

infatti, tra crimini internazionali e comportamenti che sono *sic et simpliciter* contrari alle norme internazionali.[65] A riprova, viene invocata la circostanza per cui nessun tribunale internazionale esistente avrebbe mai condannato né imputato nessuno per operazioni di spionaggio *per se* considerate.[66] Tuttavia, in un contesto di riluttanza degli Stati ad ammettere l'esistenza di attività spionistiche, di diffusione di soluzioni stragiudiziali del tipo *tit for tat*,[67] e di assenza di precedenti giurisprudenziali, l'argomentazione non appare solida.

La terza elaborazione dottrinale si limita ad osservare l'ambiguità intrinseca nell'attività di spionaggio. Ai sensi del diritto internazionale sarebbe impossibile classificarla come lecita o illecita in termini assoluti.[68] Questa dottrina si sofferma su come lo spionaggio venga condotto per ragioni di legittima difesa e per interessi propri dello Stato che invia l'agente.[69] La mancanza di trattati in materia sarebbe solo un'ulteriore conferma a favore dell'orientamento in esame.[70]

Secondo questo c.d. "approccio funzionale", in sostanza, la mancanza di un consenso sul piano internazionale impedisce la formazione di norme consuetudinarie.[71] Data la persistenza del vuoto normativo, è ragionevole dedurre che gli Stati siano più inclini a protrarre la pratica. Questo sia per garantire il proprio benessere, [72] che per tutelarsi dagli altri membri della comunità internazionale che parimenti autorizzano operazioni di spionaggio.

Sempre prescindendo da valutazioni di liceità, l'approccio funzionale si ricollega alla teoria accennata *supra*, secondo la quale lo spionaggio sarebbe l'imprescindibile strumento della legittima difesa preventiva. [73] Si deve riconoscere che un'efficace attività di *intelligence* può limitare notevolmente il

---

[65] I DELUPIS, *op. cit.* 68; A J RADSAN, *op.cit.* 605.
[66] *Ibidem*, vengono citati tra tutti i tribunali di Norimberga e de L'Aia.
[67] *Cfr.* §2.4.
[68] D B SILVER, F P HITZ & J E SHREVE ARIAIL, *Intelligence and Counterintelligence*, in *National Security Law* (J N Moore & R F Turner, 2nd edn, 2005) 935, 965.
[69] *Cfr. supra* § 2.2.1.
[70] *Ibidem*; *"all developed nations, as well as many lesser-developed ones, conduct spying and eavesdropping operations against their neighbors"*: C D BAKER, *op. cit.* 1091.
[71] C D BAKER, *op. cit.* 1095.
[72] *Ibidem*.
[73] *Ibidem*; Q WRIGHT, *op. cit.* 17-18; *cfr.* con quanto sostenuto dal Segretario di Stato USA in merito allo *U-2 Incident*, riguardo alle ricognizioni aeree. "*The Government of the United States would be derelict to its responsibility not only to the American people but to free peoples everywhere if it did not, in the absence of Soviet cooperation, take such measures as are possible unilaterally to lessen and to overcome this danger of surprise attack*": Dept. of State Bulletin (23/05/1960) 816-817.

rischio di violazioni dello *jus ad bellum*, ed al contempo rendere possibile l'applicazione effettiva del principio di proporzionalità durante un conflitto armato.[74]

Inoltre, se non si permettesse agli Stati di raccogliere le informazioni necessarie, la legittima difesa sarebbe impossibile in casi di attacco a sorpresa o con brevissimo preavviso.[75]

1.3. Soluzioni proposte

Le conclusioni tratte dalla dottrina sono utili se si vuole disegnare un quadro generale sullo spionaggio. L'approccio funzionale, in particolar modo, ha il pregio di non fermarsi a mere dichiarazioni di principio. Dovendo accettare il vuoto normativo che affligge l'intera materia, esso si concentra sulla pratica degli Stati cercando di trarne spunti costruttivi. Anche la tesi a sostegno della liceità dello spionaggio giunge essenzialmente a conclusioni analoghe, sfumando i confini fra i due orientamenti.

La seconda dottrina può certamente essere accolta nella parte in cui condanna la violazione della sovranità territoriale, conseguenza di qualsiasi operazione di spionaggio. Si può aggiungere che le operazioni di *intelligence* e spionaggio non risulterebbero in linea con i principi codificati nella Risoluzione dell'Assemblea Generale dell'ONU del 24 Ottobre 1970.[76] Il difetto più rilevante della presente dottrina è quello di condannare l'attività di spionaggio in sé, dato che nulla in merito è affermato dalle norme convenzionali o consuetudinarie.

Tutte le posizioni precedenti sono accomunate da uno stesso limite: tentare un approccio olistico in relazione ad una fattispecie che invece è composita e mutevole. Dunque, si suggerisce di adottare un approccio pragmatico che, caso per caso, si prefigga di osservare come e in quale tipo di attività si sia manifestata l'operazione di spionaggio.

---

[74] Ad esempio, è grazie all'*intelligence* che viene segnalata ai belligeranti la presenza di civili od altri obiettivi vietati nella zona di contatto.

[75] C D BAKER, *op. cit.* 1096; "*[S]pying may serve the common-interest function of warning the spying State of the other's preparations for surprise attack*": J STONE, "Legal Problems of Espionage in Conditions of Modern Conflict", in *Essays on Espionage and International Law*, *op. cit.* 42.

[76] A/RES/2625(XXV): Dichiarazione relativa ai principi di diritto internazionale, concernente le relazioni amichevoli e la cooperazione tra gli Stati, in conformità con la Carta delle Nazioni Unite.

Le violazioni delle quali può rendersi colpevole la spia sono essenzialmente le seguenti:

1) Ingerenza nella sovranità territoriale di uno Stato: è la violazione più comune. Nei paragrafi *infra* si affronterà anche la questione dell'attività di *intelligence* compiuta in spazi non soggetti alla sovranità di alcuno.
2) Abuso delle immunità diplomatiche: qualora la spia sia accreditata come agente diplomatico.[77]
3) Violazione di sedi diplomatiche: qualunque forma di spionaggio o *intelligence gathering* in contrasto con il dettato dell'Art. 22(1) della Convenzione di Vienna del 1961 sulle relazioni diplomatiche.[78]
4) Gravi violazioni dei diritti umani alla *privacy* e alla tutela dei dati personali: si tratta del caso in cui la raccolta di informazioni sia condotta in modo massiccio ed indiscriminato.

È opportuno fare delle considerazioni. Teoricamente, ognuno dei punti precedenti è eventuale e defettibile. Tuttavia, è difficile ipotizzare un caso di spionaggio che non comporti un'intrusione. E anche qualora la spia si fosse introdotta lecitamente nel territorio dello Stato del *target*, esiste una regola fondamentale riconosciuta dalla giurisprudenza internazionale:[79] non solo è proibito l'ingresso non autorizzato nel territorio straniero, ma anche l'utilizzo non autorizzato di quel territorio.[80] Al contrario, è perfettamente possibile compiere attività di *intelligence* in senso lato senza intrusione o ingerenza alcuna, soprattutto nella forma della SIGINT.

La distinzione appena fatta permette di arrivare ad una prima conclusione: l'*intelligence gathering* può essere posta in essere senza commettere alcuna violazione del diritto internazionale. Al contrario, quando anche lo spionaggio in

[77] *Cfr.* § 2.5 *infra*.
[78] *Cfr.* § 2.7 *infra*; l'Art. 22(1) recita: " Le stanze della missione sono inviolabili. Senza il consenso del capomissione, è vietato agli agenti dello Stato accreditatario accedere alle stesse".
[79] *Lotus Case* (France v Turkey) Merits [1927] PCIJ.
[80] Per "utilizzo non autorizzato", deve intendersi l'esercizio di poteri sovrani non autorizzato. Vd. S CHESTERMAN, *op. cit.* il quale fa riferimento anche alle c.d. *extraordinary renditions*, citando il caso di Abu Omar. Nel 2003, l'*Imam* egiziano fu sequestrato a Milano da agenti della CIA, a quanto risulta senza alcuna autorizzazione da parte delle autorità italiane.

sé è ritenuto lecito,[81] durante l'esecuzione della missione la spia si renderà inevitabilmente colpevole di almeno uno degli illeciti elencati.

Una critica ulteriore va mossa specificatamente all'approccio funzionale, nella parte in cui fa discendere la liceità dello spionaggio dal diritto alla legittima difesa ex Art. 51 della Carta delle Nazioni Unite. Le recenti rivelazioni di Edward Snowden,[82] infatti, dimostrano come *intelligence* e spionaggio siano indirizzati non solo verso *target* ostili o quantomeno "sospetti", ma anche verso alleati storici.

Nemmeno è da accogliere l'asserzione dei "funzionalisti"[83] secondo cui la disponibilità di informazioni ottenute con l'*intelligence* sarebbe un incentivo per gli Stati a siglare trattati.[84] Essi sostengono che tale canale sia meno soggetto a frodi e manipolazioni, rafforzando la reciproca fiducia tra gli Stati.[85]

Simili conclusioni non sembrano essere accettabili. Sostenere la validità dell'*intelligence* come strumento di monitoraggio è discutibile. Anzitutto, è difficile considerare in buona fede le parti di una convenzione, se spinte dall'incentivo di poter verificare clandestinamente il rispetto delle previsioni. *A latere*, volendo fornire un'argomentazione più logica che giuridica, sembra paradossale affermare che attraverso l'attività di *intelligence* si accresca la fiducia reciproca tra gli Stati.

2. Operazioni condotte in luoghi non soggetti a sovranità

Senza l'intrusione fisica del *case officer*, si è detto, non può parlarsi propriamente di spionaggio. Eppure, è certamente possibile ottenere risultati analoghi (i.e. l'acquisizione di informazioni classificate o comunque riservate, senza il consenso dello Stato *target*) attraverso la SIGINT o altre forme di *intelligence*. Spesso nella pratica, come si vedrà, il momento specifico della raccolta delle informazioni ha luogo in spazi non soggetti alla sovranità di alcuno,

[81] *Cfr.* §§ 2.2.1, 2.2.3.
[82] *Cfr.* Capitolo III *infra*.
[83] C D BAKER, *op. cit.*; R J STANGER, "Espionage and Arms Control" in *Essays on Espionage and International Law*, *op. cit.*; K W ABBOTT, "«Trust but Verify»: The Production of Information in Arms Control Treaties and Other International Agreements" (1993) 26 Cornell Int'l L J 23-24; L K JOHNSON, "Spies" [Sett 2000] Foreign Pol'y 25.
[84] *Cfr.* C D BAKER, *op. cit.* vengono presi ad esempio trattati inerenti la sicurezza internazionale quali il CTBT e la *Proliferation Security Initiative* (PSI) del 2003.
[85] C D BAKER, *op. cit.* 1102-1111.

siano essi l'alto mare o lo spazio aperto. Il beneficio principale ed evidente che ne deriva è la sottrazione dell'*actus reus* alla giurisdizione territoriale dello Stato sovrano sorvegliato (dove in via di principio vigono leggi che puniscono penalmente *intelligence* e spionaggio). Le questioni di diritto internazionale che ne scaturiscono sono molteplici, dalla responsabilità dello Stato mandante all'entità dell'illecito. Di seguito, attraverso la disamina di alcuni degli incidenti più rilevanti in tema di sorveglianza transnazionale, si cercherà di analizzare la materia.

2.1. SIGINT in alto mare: l'incidente della *U.S.S. Pueblo*

L'incidente internazionale che coinvolse la *Pueblo* risale al 1968. Si tratta di una nave della marina statunitense equipaggiata con armamenti leggeri ed impiegata primariamente nella raccolta di *intelligence* dei segnali elettronici. Fu attaccata (senza preavviso, almeno attenendosi alle fonti) da navi da guerra nordcoreane e costretta ad attraccare al porto di *Wonsan*. La distanza della *Pueblo* dalle coste nordcoreane al momento della cattura è incerto. Le fonti statunitensi indicano 15 NM, quelle nordcoreane meno della metà (7,1 NM). L'equipaggio fu tenuto prigioniero per circa undici mesi. Per liberare i propri connazionali, il negoziatore del governo degli Stati Uniti accettò di firmare una dichiarazione di scuse predisposta dalla Corea del Nord. In questa, si riconosceva che le attività di spionaggio e di intrusione nelle acque territoriali nordcoreane erano illegali. Pertanto, la marina nordcoreana aveva agito in legittima difesa. Contemporaneamente, il governo statunitense ritrattava ogni punto.[86]

L'evento solleva ancora oggi diverse questioni giuridiche. Per poter affrontare quelle relative alla raccolta di *intelligence*, non si può prescindere dalla controversia nata in merito all'estensione delle acque territoriali della Corea del Nord. Infatti, è necessario appurare se la *Pueblo* si trovasse effettivamente in alto mare (come sostenuto dagli USA) o meno.

[86] G H WOODWARD, "Release of the Crew of the U.S.S. Pueblo" [1969] 8 I L M 198; per un'analisi esaustiva dell'incidente, vd. X H OYARCE, "Pueblo Incident (1968)" [2007] Max Planck Encyclopedia of Public International Law §B: http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1210?rskey=jONnuq&result=1&prd=EPIL.

La Corea del Nord, dal canto suo, ha sempre sostenuto in maniera coerente che le proprie acque territoriali si estendono per 12 NM. L'unico punto di incertezza è costituito dalla veridicità delle dichiarazioni che collocavano la *Pueblo* a 7,1 NM dalla costa al momento dell'attacco. Gli Stati Uniti tenevano una posizione più ambigua. Asserivano che la *Pueblo* aveva il preciso ordine di tenersi a 15 NM dalla costa nordcoreana. Al tempo stesso, sostenevano di non aver ricevuto nessuna dichiarazione ufficiale in merito all'estensione delle acque territoriali rivendicate dalla Corea del Nord, ritenendo conseguentemente applicabile il limite consuetudinario di 3 NM.[87] Premettendo che senza un accertamento giudiziale dei fatti ci si può limitare alla semplice congettura, si analizzeranno due diverse ipotesi.

Se effettivamente la *Pueblo* si trovava nelle acque territoriali nordcoreane, bisogna capire se il passaggio fosse inoffensivo o meno. Innanzitutto, *nulla quaestio* sul fatto che la *Pueblo* fosse una nave da guerra.[88] Era armata di due mitragliatrici e condotta da un equipaggio vestito delle uniformi della *U.S. Navy*.[89] La circostanza in sé non crea particolari problemi, giacché secondo la Convenzione di Ginevra del 1958, "tutte le navi" godono del diritto di passaggio inoffensivo.[90] Vi sono però diverse condizioni da applicare. *In primis*, il passaggio deve essere "continuo e rapido", salvo situazioni d'emergenza o forza maggiore.[91] Ancora, il passaggio non deve recare pregiudizio "alla pace, al buon ordine o alla sicurezza dello Stato costiero".[92] Stando alle affermazioni dei rappresentanti del governo nordcoreano, gli USA avrebbero violato entrambe le disposizioni, fermando il natante entro le 7,1 NM per svolgere attività di *intelligence*.[93] Supponendo, nuovamente, che l'accertamento dei fatti sia accurato,

[87] Si deve tenere a mente che nel 1968 non esistevano ancora norme comunemente riconosciute in materia di confini marittimi. La Convenzione di Ginevra sul Mare Territoriale e la Zona Contigua del 1958, poneva solo un limite massimo di 12 NM per la Zona Contigua. La UNCLOS entrerà in vigore soltanto nel 1994; X H OYARCE, *op. cit.* §C(1).
[88] *Cfr.* R E COYLE, "Surveillance From the Seas" [1973] 75 Mil L Rev 82; non è condivisibile la tesi opposta, per cui "*the Pueblo is not a warship but a vessel whose raison d'être is espionage, even if she is made to look like a warship*": C C MORRISSON, "International Law and the Seizure of the USS Pueblo" (1968) 4 Tex Int'l L F 191.
[89] X H OYARCE, *op. cit.* §B.
[90] Convenzione di Ginevra sul Mare Territoriale e la Zona Contigua del 1958, Sezione III A; *cfr. Corfu Channel, U.K. v Albania*, (Judgment) [1948] ICJ 15.
[91] Convenzione di Ginevra sul Mare Territoriale e la Zona Contigua del 1958, Art. 14(3).
[92] *Ibidem*, Art. 14(4).
[93] X H OYARCE, *op. cit.* §C(2).

l'interpretazione pare corretta. [94] All'epoca forse si poteva discutere sull'"innocenza" o meno dell'attività di SIGINT.[95] Tuttavia, oggi la UNCLOS è chiara nello statuire che "*any act aimed at collecting information to the prejudice of the defence or security of the coastal State*" rende il passaggio della nave pregiudizievole della pace, buon ordine o sicurezza dello Stato costiero.[96]

Ipotizzando ora invece che la *U.S.S. Pueblo* si trovasse in alto mare (i.e. a 15 NM), lo scenario è sostanzialmente diverso. Innanzitutto la cattura sarebbe stata illecita ex Art. 8(1) della Convenzione Concernente l'Alto Mare.[97] Questa, riconoscendo il diritto consuetudinario vigente,[98] stabilisce che le navi da guerra, in alto mare, godono "dell'immunità di giurisdizione da parte degli Stati diversi da quello della bandiera." Neppure pare applicabile il diritto all'inseguimento ex Art. 23 della Convenzione in parola,[99] per due motivi. Anzitutto l'attività di SIGINT, in questa ricostruzione, è stata iniziata e proseguita sempre in alto mare. Inoltre, non esiste un precedente nel diritto penale di alcuno Stato che collochi la fattispecie tra quelle punite come spionaggio (od in forza di qualsiasi altra norma penale).[100]

Ciò che si evince dal caso in esame è coerente con quanto affermato finora sull'*intelligence* diversa dallo spionaggio. La raccolta di informazioni non si può dire illecita *per se*, dal momento che non c'è alcuna intrusione che possa turbare la sovranità territoriale dello Stato sorvegliato.[101] Neanche una nave da guerra perde la propria immunità, a patto che la raccolta avvenga in alto mare. In caso contrario (vale a dire per SIGINT raccolta nelle acque territoriali dello Stato costiero) si perde il diritto al passaggio inoffensivo.[102]

---

[94] Al contrario, fintantoché la lettura di segnali elettronici è funzionale alla navigazione è ammissibile, *cfr.* R E COYLE, *op. cit.* 86.
[95] R E COYLE, *op. cit.* 85.
[96] *United Nations Convention on the Law of the Sea*, Montego Bay 1982, Art. 19(2)(c); vd. anche il commento alla posizione tenuta dal Segretario di Stato Rusk a seguito dell'incidente: A P RUBIN, "The Impact of the Pueblo Incident in International Law" (1969-1970) 49 Or L Rev 7.
[97] Convenzione di Ginevra Concernente l'Alto Mare del 1958; G H ALDRICH, "Questions of International Law Raised by the Seizure of the U.S.S. Pueblo" 63 Am Soc'y Int'l L Proc 3.
[98] *Cfr.* X H OYARCE, *op. cit.* §C3(b).
[99] "L'inseguimento d'una nave straniera può essere operato solo se le autorità competenti dello Stato costiero hanno motivo di credere che detta nave abbia contravvenuto a leggi o regolamenti di questo Stato."
[100] G H ALDRICH, *op. cit.* 5.
[101] A P RUBIN, *op. cit.* 10.
[102] X H OYARCE, *op. cit.* §D.

La recente prassi anglo-americana, consistente nella raccolta indiscriminata e massiccia di dati personali (si fa riferimento a programmi quali PRISM e *Tempora*) solleva nuove questioni. *Quid juris* se la nave, sia essa da guerra o meno, pur trovandosi in alto mare raccogliesse in massa segnali elettronici provenienti dallo Stato costiero? In questa peculiare situazione, esistono i presupposti per riconoscere una violazione delle norme internazionali a tutela di *privacy* e dati personali come diritti umani.[103] L'immunità della "nave-spia"[104] rimarrebbe sempre valida, ma sembrerebbe possibile invocare la responsabilità dello Stato di bandiera.

Il COYLE suggerisce un ulteriore spunto.[105] L'autore, pur concordando sulla liceità *per se* della sorveglianza in alto mare, realizza d'altro canto che l'*intelligence* è sempre strumentale ad uno scopo. Si dovrebbe allora distinguere di volta in volta: se le informazioni sono dirette ad uno scopo lecito, l'attività di sorveglianza rimane lecita. Se le informazioni servono uno scopo illecito (es. propaganda ostile all'interno dello Stato costiero), anche la sorveglianza è illecita.[106] Pur precedendo di diversi anni il *datagate*, questa opinione può raccordarsi con quanto appena detto in merito all'*intelligence* massiccia ed indiscriminata: quando la sorveglianza è diretta ad una violazione dei diritti umani, costituisce un illecito a sua volta.

2.2. Ricognizione area: l'incidente dello U-2

Questo secondo incidente internazionale riguarda l'abbattimento di un aereo ricognitore statunitense (modello U-2, per l'appunto) mentre sorvolava senza autorizzazione il suolo sovietico. Avveniva nel Maggio 1960, durante la Guerra Fredda. La vicenda fu sottoposta all'attenzione del Consiglio di Sicurezza dell'ONU tra il 23 ed il 26 Maggio del medesimo anno. In modo singolare, gli USA non negarono di aver condotto voli finalizzati alla raccolta di *intelligence*.[107] La posizione statunitense in merito fu quella di rivendicare la legittimità del

[103] Per una trattazione completa, vd. *infra*.
[104] Il termine qui non è usato in senso tecnico. Si ricorda che l'attività di cui al presente paragrafo è di SIGINT e non di spionaggio.
[105] R E COYLE, *op. cit.* 94.
[106] *Ibidem*.
[107] Q WRIGHT, "Legal Aspects of the U-2 Incident" [1960] 54 Am J Int'l 836.

programma di ricognizioni U-2, giustificata dalla necessità di conoscere il potenziale militare dell'URSS. Ciò per poter efficacemente esercitare il diritto alla legittima difesa contro attacchi improvvisi. Tuttavia, per questioni prettamente politiche, gli Stati Uniti promisero di sospendere il programma degli U-2.

Andrej Gromyko, rappresentante dell'Unione Sovietica, propose la seguente *draft resolution*, poi respinta:

> *The Security Council*
>
> Having examined *the question of "Aggressive acts by the Air Force of the United States of America against the Soviet Union, creating a threat to universal peace,"*
>
> Noting *that violations of the sovereignty of the state are incompatible with the principles and purposes of the Charter of the United Nations,*
>
> Considering *that such actions create a threat to universal peace,*
>
> *1.* Condemns *the incursions by the United States aircraft into other states and regards them as aggressive acts;*
>
> *2.* Requests *the Government of the United States of America to adopt immediate measures to halt such actions and to prevent their recurrence.*

La condanna della Russia sovietica si basava su due punti. In primo luogo, le incursioni aeree costituiscono una violazione della sovranità territoriale. Inoltre, queste sono classificabili come atti di aggressione e perciò comportano una minaccia alla pace ed alla sicurezza internazionale. Se questo secondo punto fu quasi unanimemente respinto dagli Stati membri del Consiglio di Sicurezza,[108] in modo altrettanto compatto fu accolta la prima dichiarazione.[109] Infatti, tutte le convenzioni sull'aviazione vigenti all'epoca (e la situazione odierna non è differente) proibivano il sorvolo non autorizzato di aerei stranieri.[110] Lo spazio aereo è sottoposto alla sovranità "piena ed esclusiva" dello Stato territoriale sottostante.[111] Per di più, lo U-2 in questione può essere classificato come "aeromobile di Stato", per il quale il sorvolo è proibito salvo autorizzazione "data

[108] Ciò è peculiare, se si ricorda che la Risoluzione dell'Assemblea Generale sulla Definizione di Aggressione 3314 (XXIX) sarà adottata solo nel 1976.
[109] Q WRIGHT, *op. cit.* 842.
[110] Convenzione de l'Avana del 1928; Convenzione di Chicago sull'Aviazione Civile Internazionale del 1944, Art. 3(c); *cfr.* Convenzione di Parigi del 1919, Art. 5 (di cui gli USA non sono parte).
[111] Convenzione di Chicago del 1944, Art. 1.

mediante accordo speciale o in altro modo e conformemente alle condizioni di tale autorizzazione."[112]

Dalle considerazioni appena fatte si evince che l'*intelligence* mediante osservazioni aeree ha molto in comune con lo spionaggio. In entrambi i casi, l'atto della raccolta di informazioni non può dirsi illecito, ma le modalità d'esecuzione comportano una inaccettabile intrusione nel territorio di uno Stato sovrano.

Anche per quanto riguarda le contromisure che lo Stato osservato può adottare, vale quanto detto in merito allo spionaggio. L'agente (in questo caso il pilota del velivolo) sarà sottoposto alla giurisdizione penale dello Stato spiato e potrà invocarsi la responsabilità internazionale dello Stato mandante. Invece, pare inaccettabile la reazione dell'URSS che nel caso di specie impiegò la forza armata per abbattere il ricognitore.[113] L'attività di *intelligence*, infatti, in nessun modo giustifica l'uso della forza. Neppure nei modi consentiti ex. Art. 51 della Carta delle Nazioni Unite.[114] Né vengono rispettati i criteri stabiliti nel celebre caso *Caroline*, per cui l'uso della forza in legittima difesa è ammissibile quando costituisce "*instant and overwhelming necessity, permitting no choice of means and no moment for deliberation*".[115]

Volendo attualizzare la questione, ci si può chiedere se voli di ricognizione, analoghi a quello in esame, siano ammissibili oggi in forza del Trattato sui Cieli Aperti del 1992. La risposta, essenzialmente, è negativa.[116] Infatti, se pure il Trattato consente di effettuare voli d'osservazione sui territori dei vari Stati membri,[117] di certo la raccolta di *intelligence* non è ricompresa nello scopo dello strumento normativo. La finalità del Trattato è la trasparenza, anche per quanto riguarda il potenziale militare, tra Stati membri. Tuttavia, l'*intelligence gathernig* è ben diversa dalla semplice osservazione autorizzata dal *target*. La segretezza è un elemento fondamentale, tanto nel momento della raccolta dell'informazione, quanto nell'oggetto della raccolta. È forse anche per questo motivo che "[l]a Parte

[112] *Ibidem*, Art. 3(c).
[113] Q WRIGHT, *op. cit.* 836.
[114] *Ibidem*, 851.
[115] J B MOORE, *Digest of International Law* (Washington DC, 1906) 412.
[116] RONZITTI N., *op. cit.*
[117] Trattato sui Cieli Aperti del 1992, Art. I(1): "Il presente Trattato stabilisce il regime, che sarà denominato regime Cieli Aperti, per l'effettuazione di voli d'osservazione da parte degli Stati Parte sui territori di altri Stati Parte ed enuncia i diritti e gli obblighi degli Stati Parte riguardo a tale regime."

osservata avrà il diritto di vietare un volo d'osservazione che non sia conforme alle disposizioni del presente Trattato."[118]

Il discorso cambia quando la sorveglianza aerea è svolta nello spazio aperto. Gli USA ad esempio, già tra il 1960 ed il 1966, intraprendevano il programma dei satelliti *Samos-Midas* per controllare l'attività missilistica dell'URSS.[119] Diversi altri ne esistono ad oggi, per gli scopi più vari ma comunque correlati all'*intelligence gathering*.[120] Analogamente a quanto detto in merito all'alto mare, bisogna tenere a mente che gli spazi cosmici non sono soggetti alla sovranità di alcuno.[121] Nella prassi internazionale, nessuno Stato ha mai riconosciuto l'obbligo di chiedere il consenso di altri Paesi per il sorvolo di satelliti e velivoli della stessa specie.[122] Perciò, seguendo le conclusioni raggiunte circa l'*intelligence* in alto mare, bisogna pensare che neanche in questo diverso caso si configuri una violazione della sovranità territoriale. Conseguentemente, l'attività in sé considerata è lecita. Vale altresì quanto sostenuto in merito alla *bulk data collection*: integrando una violazione dei diritti umani, è inaccettabile pure quando le modalità di raccolta dei dati sono di per sé leciti.

3. Spionaggio da parte di agenti diplomatici

La situazione è ben diversa quando la spia è stata accreditata come agente diplomatico.[123] Di questo fenomeno si hanno diverse testimonianze risalenti al periodo della Guerra Fredda, tanto da parte di agenti USA che sovietici.[124] La

---

[118] *Ibidem*, Art. VIII(1).
[119] Q WRIGHT, J S STONE, R A FALK & R J STANGER, *Essays on Espionage and International Law* (Ohio State University Press, 1962) 45ss.
[120] P KORODY, "States Surveillance Within U.S. Borders" [2004] 65 Ohio St L J 1627.
[121] CONFORTI B., *op. cit.* 323.
[122] *Ibidem*; vd. anche il Trattato sui Principi Relativi alle Attività degli Stati in Materia di Esplorazione ed Utilizzazione dello Spazio Extra-Atmosferico, Inclusi la Luna e Altri Corpi Celesti del 1967,
[123] C FORCESE, *op. cit.* 200-201; A S HULNICK, *op. cit.* 167; N GRIEF, "The Take-Over of the United States' Embassy in Tehran**:** Some Questions of Diplomatic Law" (1980) 13 B L J 52-53; non viene qui riportata la distinzione tra *case officers* "legali" (accreditati come diplomatici) ed "illegali" (non accreditati), perché priva di reale valenza giuridica: J RADSAN, *op. cit.* 344.
[124] La prassi coinvolge altresì delegati e personale delle Nazioni Unite: vd. *United States v Melekh* [1960] 190 F Supp 67; *United States v Drummond* [1965] 354 F 2d 132; *United States v Butenko* [1967] 384 F 2d 554, 556; N P WARD, *op. cit.* 670. Vd. anche la *National HUMINT Collection Directive* del 2009, con la quale il Dipartimento di Stato USA demandava ai propri diplomatici operazioni di spionaggio sugli ufficiali delle Nazioni Unite. Il testo è stato pubblicato dal sito *Wikileaks*: http://www.wikileaks.org/cable/2009/07/09STATE80163.html.

ratio alla base di una simile pratica è evidente: dal momento che il diplomatico gode dell'immunità dalla giurisdizione penale e civile, la spia accreditata non sarà perseguibile dallo Stato accreditatario.[125]

A questo proposito si richiama il dettato della Convenzione di Vienna sulle relazioni diplomatiche del 1961 (CVRD), comunemente considerata essere ricognitiva del diritto internazionale consuetudinario.[126] Le immunità diplomatiche, a ben vedere, rivestono un ruolo cruciale nel pacifico mantenimento delle relazioni internazionali fra paesi.[127]

In primis, l'articolo 29 della Convenzione sancisce che:

> La persona dell'agente diplomatico è inviolabile. Egli non può essere sottoposto ad alcuna forma di arresto o di detenzione. Lo Stato accreditatario lo tratta con il rispetto dovutogli e provvede adeguatamente a impedire ogni offesa alla persona, libertà e dignità dello stesso.[128]

L'Articolo 31(1) integra quanto affermato sopra. In particolare il primo paragrafo specifica che "[l]'agente diplomatico gode dell'immunità dalla giurisdizione penale dello Stato Accreditatario".[129] Tale limite alla potestà dello Stato ricevente

---

[125] E.g. l'immunità fu negata a due agenti segreti del governo francese che avevano affondato la nave *Rainbow Warrior*; vd. *Rainbow Warrior (New Zeland v France)* [1990] France-New Zeland Arbitration Tribunal; *cfr.* RONZITTI N., *Introduzione al Diritto Internazionale* (Giappichelli, 4a edn, 2013) 148.

[126] *Cfr. Case Concerning Diplomatic and Consular Staff in Tehran* (24 May 1980) ICJ; CURTI GIALDINO C., *Lineamenti di Diritto Diplomatico e Consolare* (Giappichelli, 2a edn, 2014) 223-224.

[127] Convenzione di Vienna sulle relazioni diplomatiche 1961 (Preambolo) periodi terzo e quarto; N GRIEF, *op. cit.* 47, 55.

[128] *Cfr.* CURTI GIALDINO C., *op. cit.* 224-225. Si tratta della codificazione di una consuetudine millenaria, che può essere fatta risalire all'epoca dei Fenici e degli antichi Egizi per i quali gli ambasciatori rivestivano un ruolo sacro. Nel Digesto, POMPONIO recita: "*[s]i quis legatum hostium pulsasset, contra ius gentium id commissum esse existimantur, quia sancti habentur legati*". I primi tentativi di trasporre la regola in una norma scritta sono la Convenzione de L'Avana del 1928 (Art. 14), la Risoluzione sulle Immunità Diplomatiche dell'*Institut de Droit International* del 1929 (Art. 7) e il progetto della *Harward Law School* del 1932 (Art. 17); vd. anche la Convenzione sulla Prevenzione e la Repressione dei Reati Contro le persone internazionalmente Protette, compresi gli Agenti Diplomatici del 20 febbraio 1977: si tratta di uno strumento predisposto dalla ILC su impulso dell'Assemblea Generale delle Nazioni Unite. Fu ritenuto necessario a fronte del moltiplicarsi di attentati e altri atti compiuti ai danni di diplomatici nel corso degli anni '60; *cfr.* CURTI GIALDINO C., *op. cit.* 230.

[129] I periodi successivi contengono delle (limitatissime) eccezioni al principio sopra esposto; vd. Convenzione di Vienna del 1961, Art. 31(1): "[l]'agente diplomatico gode dell'immunità dalla giurisdizione penale dello Stato accreditatario. Esso gode del pari dell'immunità dalla giurisdizione civile e amministrativa dello stesso, salvo si tratti di:
a. azione reale circa un immobile privato situato sul territorio dello Stato accreditatario, purché l'agente diplomatico non lo possegga per conto dello Stato accreditante ai fini della missione;
b. azione circa una successione cui l'agente diplomatico partecipi privatamente, e non in nome dello Stato accreditante, come esecutore testamentario, amministratore, erede o legatario;

è di tipo strettamente personale.[130] Si tratta, in sostanza, di una misura dal carattere puramente processuale che risponde all'esigenza "*ne impediatur legatio*".[131] È quanto riconosceva e.g. la *House of Lords* nel 1930, nel caso *Dickinson v Del Solar*: "*[d]iplomatic privileges does not import immunity from legal liability but only exemption from legal jurisdiction*".[132] Venute meno le prerogative che avevano giustificato la concessione dell'immunità (i.e. lo status di diplomatico), l'individuo torna ad essere soggetto alla giurisdizione penale e civile dello Stato accreditatario.[133] Si noti che immunità non è sinonimo di impunità: ex Art. 31(4) CVRD ben potrebbe lo Stato accreditante giudicare l'agente per atti compiuti nel corso della missione (anche prima che questa sia cessata). La condizione, ovviamente, è che il fatto sia preveduto come reato anche in patria.[134]

L'Articolo 39(2) della Convenzione in parola fornisce una tutela ulteriore all'agente accreditato: per gli atti compiuti nella veste di organo dello Stato, l'immunità perdura anche dopo la cessazione delle funzioni. Si tratta della c.d.

---

c. azione circa un'attività professionale o commerciale qualsiasi, esercitata dall'agente diplomatico fuori delle sue funzioni ufficiali nello Stato accreditatario"; vd. anche *Ibidem*, Art. 31(3): "[c]ontro l'agente diplomatico non può essere presa alcuna misura d'esecuzione, salvo nel casi di cui al paragrafo 1, capoversi a a c, purché non ne sia menomata l'inviolabilità della persona e della dimora"; *cfr.* A ATTERITANO, "Immunity of States and Their Organs: The Contribution of Italian Jurisprudence Over the Past Ten Years" [2009] 19 Italian Y B Int'l L 54-55.

[130] Da cui il nome di "immunità personali" o "*ratione materiae*"; *cfr.* CONFORTI B., *op. cit.* 261.

[131] *Ibidem*.

[132] *Dickinson v Del Solar* [1930] 1 KB 376; *cfr.* E DENZA, *op. cit.* 286; tra l'altro, è sempre possibile la celebrazione del processo qualora lo Stato accreditante decida di spogliare il diplomatico della propria immunità: CURTI GIALDINO C., *op. cit.* 235, 241-243; vd. RONZITTI N., *op. cit.* 152: "da un punto di vista strettamente giuridico, titolare del diritto soggettivo all'immunità è lo Stato accreditante. Ne consegue che solo lo Sato accreditante può, ove lo ritenga opportuno, rinunziare all'immunità dei suoi agenti diplomatici dalla giurisdizione locale."

[133] Vd. Convenzione di Vienna del 1961, Art. 39(2): "[i] privilegi e le immunità di una persona che cessa dalle sue funzioni, decadono ordinariamente al momento in cui essa lascia il paese oppure al decorso d'un termine ragionevole che le sia stato concesso, ma sussistono fino a tale momento anche in caso di conflitto armato […]"; sulla cessazione delle immunità vd. E DENZA, *op. cit.* 434 (citando Vattel): "*ses fonctions cessent mais ses privilèges et ses droits n'expirent point dès ce moment: il les conserve jusqu'à son retour auprès du maître è a qui il doit rendre compte de son ambassade, dans le départ que dans la venue*".

[134] CURTI GIALDINO C., *op. cit.* 236; *cfr. Case concerning the arrest warrant of 11 April 2000* (DRC v. Belgium) Merits, Judgment of 14 February 2002 §60: "*immunity from criminal jurisdiction and individual criminal responsibility are quite separate concepts. While jurisdictional immunity is procedural in nature, criminal responsibility is a question of substantial law. Jurisdictional immunity may well bar prosecution for a certain period or for certain offences; it cannot exonerate the person to whom it applies from all criminal responsibility*".

"immunità funzionale".[135] Gli atti ufficiali si considerano a tutti gli effetti come atti dello Stato accreditante e dunque, secondo la regola generale, nessun diplomatico può essere citato in giudizio con riferimento ad essi.[136] Dovendosi applicare unicamente agli atti compiuti nell'esercizio di funzioni ufficiali, sorgono serie perplessità circa la loro validità anche nel caso di contegni criminosi o clandestini.

La dottrina odierna, a ben vedere, nega vigorosamente una simile possibilità. Soprattutto per ciò che concerne la giurisdizione penale, è ormai pacifico che l'immunità funzionale non debba concedersi a chi si sia reso colpevole di crimini internazionali o di attività clandestine.[137] La giurisprudenza italiana fornisce un contributo concreto in materia, frutto di un'evoluzione giurisprudenziale che abbraccia gli ultimi dieci anni.

Nel caso *Abu Omar*,[138] riguardante la *extraordinary rendition* dell'omonimo Imam di Milano, il Tribunale competente in primo grado si pronunciò i.a. sulle immunità di alcuni agenti diplomatici e consolari coinvolti.[139] Innanzitutto il giudice confermò la procedibilità nei confronti dei due agenti consolari USA.[140] Questo punto è facilmente condivisibile, giacché la Convenzione di Vienna sulle relazioni Consolari del 1963 (CVRC) dispone che: "[i] funzionari consolari possono essere messi in stato d'arresto o di detenzione preventiva solamente in caso di grave delitto e per effetto d'una decisione dell'autorità giudiziaria

[135] O "immunità materiale" od anche *ratione materiae*: CONFORTI B., *op. cit.* 260; vd. A ATTERITANO, *op. cit.* 48-49; vd. Convenzione di Vienna sulle relazioni diplomatiche del 1961, Art. 39(2) ultimo periodo: "[l]'immunità sussiste tuttavia per quanto concerne gli atti compiuti da tale persona nell'esercizio delle sue funzioni come membro della missione".
[136] E DENZA, *op. cit.* 439.
[137] A ATTERITANO, *op. cit.* 55; M FRULLI, "Some Reflections on the Functional Immunity of State Officials" [2009] 19 Italian Y B Int'l L 96: "*for those purporting the existence of a general rule on the functional immunity of State organs, acts of sabotage or espionage are not covered by the rule, on the assumption that these kind of activities are carried out in the territory of a foreign State (and likely attempting at national security) without its consent.*"
[138] Tribunale di Milano (Sez. IV Penale), 1 Febbraio 2010 n. 12428.
[139] A ATTERITANO, *op. cit.* 49.
[140] Tribunale di Milano (Sez. IV Penale), 1 Febbraio 2010 n. 12428, p. 94.: "[n]on potranno invece andare esenti dalla giurisdizione penale italiana le attività compiute da Robert Seldon Lady e Sabrina De Sousa: gli stessi, come si è visto, operavano nel periodo incriminato esclusivamente come addetti consolari a Milano. Per tale categoria di persone la legge non prevede immunità in presenza di un "crime grave", come, certamente, è il reato di sequestro di persona di cui all'art. 605 c.p. in quanto la pena edittalmente prevista giunge fino a dieci anni di reclusione."

competente".[141] Le maggiori criticità sorsero con riferimento a tre agenti della CIA accreditati come diplomatici statunitensi,[142] ai quali fu riconosciuta l'immunità funzionale.[143] Tale conclusione implicava necessariamente che, almeno stando all'orientamento del giudice Magi, la *extraordinary rendition* fosse ricompresa nelle funzioni della missione ex Art. 3 CVRD.[144] Come ha notato FRULLI, in modo condivisibile, l'interpretazione del concetto di "funzione d'una missione diplomatica"[145] deve essere quanto più restrittiva possibile. È ciò che traspare dai lavori preparatori della CVRD,[146] dalla consuetudine e dalla dottrina maggioritaria.[147] Soprattutto, si pone l'accento sul fatto che lo stesso Art. 3 della Convenzione statuisce quanto segue: "[l]e funzioni d'una missione diplomatica consistono segnatamente nel: […] (b) proteggere nello Stato accreditatario gli interessi dello Stato accreditante e dei cittadini di questo, *nei limiti ammessi dal diritto internazionale*" (enfasi aggiunta).[148] *Ergo*, pur volendo ammettere per assurdo che il sequestro dell'Imam sia stato compiuto nell'esercizio del mandato diplomatico, sarebbe comunque impossibile conciliare un simile contegno con

[141] Convenzione di Vienna sulle relazioni Consolari del 25 Aprile 1963, Art. 41(1); sulla definizioe di "grave delitto" vd. la legge di attuazione della Convenzione (L. 804/1967, Art. 3): "un delitto non colposo punibile con la reclusione non inferiore a 5 anni o con pena più grave"; il Tribunale di Milano (come confermerà nel 2012 anche la Corte d'Appello) attestava che la pena prevista per i sequestro dell'Imam era pari nel minimo a dieci anni; *cfr.* CURTI GIALDINO C., *op. cit.* 409.
[142] I.e. Jeff Castelli, Ralph Enry Russomando e Betnie Medero.
[143] All'epoca del processo i tre agenti diplomatici erano già cessati dalle loro funzioni. Per questo motivo non fu invocata l'immunità personale. *Cfr*. M FRULLI, *op. cit.* 97; tra l'altro, nel corso del procedimento il GIP aveva adottato un approccio diametralmente opposto, negando l'immunità agli agenti in funzione della clandestinità delle loro azioni, vd. A ATTERITANO, *op. cit.* 55; *cfr*. GAETA P., "*Extraordinary renditions* e immunità dalla giurisdizione penale degli agenti di Stati esteri: il caso *Abu Omar*", RDI, 2006, p. 126ss.
[144] Tribunale di Milano (Sez. IV Penale), 1 Febbraio 2010 n. 12428, p. 93: "non può essere messo in dubbio che l'attività compiuta da tutti gli imputati su indicati sia stata effettuata nell'esercizio delle loro funzioni diplomatiche o consolari: diversamente da quanto ritenuto dall'ufficio del PM sul punto, ed in conformità logica con quanto già affermato in merito alla posizione del Romano, deve confermarsi che l'attività di "extraordinary renditions" compiuta dagli agenti CIA, pur costituendo reato in Italia, possa e debba sicuramente inquadrarsi nell'ambito funzionale indicato dall'art. 3 della Convenzione di Vienna ("proteggere nello Stato accreditatario gli interessi della Stato accreditante")."
[145] Convenzione di Vienna sulle relazioni diplomatiche, Art. 3(1).
[146] http://www.un.org/law/diplomaticconferences/.
[147] M FRULLI, *op. cit.* 97; la giurisprudenza in materia è piuttosto scarna, ma si attesta almeno un altro caso in cui le autorità Svizzere hanno perseguito legalmente un agente diplomatico (cessato dalle proprie funzioni) per presunti atti di spionaggio compiuti durante la missione: *cfr*. J E DONOGHUE, "Perpetual Immunity for Former Diplomats? A Response to «The Abisinito Affair: A Restrictive Theory of Diplomatic Immunity?»" (1989) 27 Colum J Transnat'l L 615, 627.
[148] Convenzione di Vienna sulle relazioni diplomatiche del 1961 Art. 3(1)(b); M FRULLI, *op. cit.*

l'Art. 3(1)(b) CVRD. In un giudizio separato,[149] la Corte d'Appello di Milano tornò a pronunciarsi sulla perseguibilità dei tre diplomatici. Seguendo un ragionamento logico-giuridico affine a quello esposto appena *supra* (e alla luce di quanto stabilito dalla Cassazione,[150] che da alcuni mesi aveva confermato la condanna nei confronti dei due agenti consolari) la Corte ribaltava il *decisum* del Tribunale:

> la Suprema Corte ha svolto un'osservazione che riguarda anche il personale diplomatico. Ha rilevato che i soggetti non hanno agito come funzionari consolari ma della CIA. Non è proprio dell'attività consolare il sequestro e la successiva tortura. L'osservazione vale, a giudizio di questa Corte, anche per il personale diplomatico […] Anche se gli odierni imputati avessero agito nell'esercizio delle loro funzioni (e si è detto che così non è), vi è il limite del diritto internazionale che non consente il riconoscimento della immunità. In definitiva bisogna verificare se l'attività svolta sia in contrasto col diritto interno. Ebbene, non c'è chi non veda come il sequestro di persona con finalità come quelle in oggetto (tortura) sia violazione dei diritti fondamentali dell'uomo.[151]

Tale pronuncia si pone ideologicamente sulla linea del caso *Pinochet*,[152] ampliandone significativamente la portata. In quella occasione la *House of Lords* inglese riconosceva che la tortura (così come qualunque altro crimine internazionale) non può rientrare nella funzione pubblica.[153] Pertanto, veniva enunciato per la prima volta il principio che è stato poi ripreso dalla giurisprudenza italiana: la definizione di "esercizio delle funzioni ufficiali" data dal paese d'origine non è vincolante per lo Stato ricevente.[154] L'avallo della CIG

[149] Per un difetto di regolarità della notifica, la questione delle immunità funzionali fu affrontata nella separata sentenza della Corte d'Appello di Milano (Sez. III Penale) 1 Febbraio 2013.
[150] Corte di Cassazione, Cass. pen., Sez. V, 19 Settembre 2012, n.46340.
[151] Corte d'Appello di Milano (Sez. III Penale) 1 Febbraio 2013, p. 35.
[152] Vd. E DENZA, *op. cit.* 444-448: arrestato nel Regno Unito sulla base di un mandato di cattura spagnolo, la difesa del Senatore Pinochet invocava l'Art. 39(2) CVRD. I crimini i.a. di omicidio e tortura che gli venivano contestati, fu sostenuto, erano stati compiuti nel corso del suo mandato come capo di Stato del Cile. Pur non rivestendo più tale carica all'epoca del processo, la persistenza delle immunità funzionali avrebbe dovuto impedire la prosecuzione del rito.
[153] Vd. opinioni dei Lord Browne-Wilkinson, Hutton e Phillips in *R v Bow Street Metropolitan Stipendiary Magistrate, ex Parte Pinochet Ugarte (No 3)* [1999] 2 WLR 827, [1999] 2 All ER 97, 119 ILR 135.
[154] E DENZA, *op. cit.* 446.

giunse solo qualche anno più tardi, nel caso noto come *Arrest Warrant Case*. Con riferimento a un mandato di cattura emesso nei confronti del Ministro degli Affari Esteri del Congo per violazioni del diritto umanitario, la Corte asserì che:

> *it is now increasingly claimed in the literature* […] *that serious international crimes cannot be regarded as official acts because they are neither normal State functions nor functions that a State alone (in contrast to an individual) can perform.*[155]

Fermo restando quanto esposto sinora, per il personale diplomatico ancora in carica sussistono pur sempre le immunità *ratione personae*.[156] Ci si interroga allora su quale sia il rimedio esperibile dallo Stato accreditatario nel caso di abusi (siano essi consistenti indifferentemente in attività clandestine o crimini internazionali). La risposta è nella "consegna dei passaporti", che comporta l'ingiunzione a lasciare entro un certo tempo il paese.[157] Essendo venuto meno il "gradimento" verso l'agente diplomatico, questi sarà dichiarato *persona non grata*.[158] Un punto di riferimento giurisprudenziale per ciò che concerne questo particolare istituto è nel cd. *Tehran Hostages Case*.[159] Gli eventi che spinsero gli Stati Uniti a presentare tale causa dinanzi alla Corte Internazionale di Giustizia sono connessi ai disordini che portarono al rovesciamento dello Shah Reza Pahlevi nel 1979.[160] Il 4 Novembre del medesimo anno, durante una manifestazione, l'ambasciata USA a Teheran fu invasa da un gruppo armato composto da centinaia di studenti musulmani.[161] Contestualmente, il personale fu preso in ostaggio ed i militanti si appropriarono degli archivi riservati della sede diplomatica.[162]

---

[155] *Case Concerning the Arrest Warrant of 11 April 2000 (DRC v Belgium)* Merits, Judgment of 14 February 2002, ICJ §85; peraltro, in quell'occasione ad essere condannato fu il Belgio, per aver violato l'immunità personale del Ministro Yerodia. Infatti, al momento della cattura questi era ancora in carica.

[156] Vd. CURTI GIALDINO C., *op. cit.* 236.

[157] CONFORTI B., *op. cit.* 259.

[158] Convenzione di Vienna sulle relazioni diplomatiche del 1961 Art. 9(1); N P WARD, *op. cit.; J* RADSAN, *op. cit.* 621; CONFORTI B., *op. cit.* 259; N GRIEF, *op. cit.* 52.

[159] *Case Concerning Diplomatic and Consular Staff in Tehran* (24 May 1980) ICJ.

[160] I BUFFARD & S WITTICH, "United States Diplomatic and Consular Staff in Tehran Case (United States of America v Iran)" [2007] Max Planck Encyclopedia of Public International Law: http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e229?rskey=J2aWjp&result=2&prd=EPIL.

[161] *Ibidem*.

[162] *Ibidem*. Il 5 Novembre accadde lo stesso anche nei consolati di Tabriz e Shiraz.

Il 29 Novembre gli Stati Uniti adirono la CIG lamentando diverse violazioni della Convenzione di Vienna sulle relazioni diplomatiche del 1961, della Convenzione di Vienna sulle relazioni consolari del 1963, nonché del trattato di amicizia firmato dalle due nazioni nel 1955.[163] La Corte, riconosciuta la propria giurisdizione in materia,[164] emise innanzitutto un *order* (datato 15 Dicembre 1979) con il quale intimava l'immediata liberazione dell'ambasciata e degli ostaggi ivi trattenuti.

Proseguendo da un lato l'occupazione e dall'altro la completa inerzia del governo iraniano, gli USA tentarono un'operazione militare di recupero. A causa di difficoltà tecniche, tuttavia, il tentativo fallì.[165] Rimaneva intanto immutata la posizione dell'Iran, che inoltre negava la giurisdizione della CIG sulla base del fatto che la rivolta degli studenti riguardava unicamente il dominio riservato dello Stato.[166] In una lettera alla Corte, il Ministro degli affari esteri iraniano ribadì che la questione degli ostaggi esprimeva solo un "*marginal and secondary aspect of an overall problem*",[167] vale a dire una serie di attività criminose che gli Stati Uniti avrebbero perpetrato in Iran per oltre venticinque anni. L'ambasciata americana veniva descritta come un centro di spionaggio e cospirazione:[168] la

[163] Treaty of Amity, Economic Relations, and Consular Rights Between the United States of America and Iran, Signed at Tehran, on 15 August 1955.

[164] La Corte riconobbe la sussistenza della propria giurisdizione sulla base di tre strumenti normativi: il I Protocollo Addizionale alla Convenzione di Vienna sulle relazioni diplomatiche, il I Protocollo addizionale alla Convenzione di Vienna sulle relazioni consolari e il *Treaty of Amity, Economic Relations, and Consular Rights* del 1955.

[165] I BUFFARD & S WITTICH, *op. cit.*; vd. *Case Concerning Diplomatic and Consular Staff in Tehran* (24 May 1980) ICJ, §93: la CIG non mancò di segnalare che l'operazione militare condotta dagli USA minava il rispetto per la Corte stessa e, in generale, per la soluzione pacifica delle controversie. Ciononostante, l'azione degli Stati Uniti non rientrava nell'oggetto del giudizio in questione. Per i dettagli della missione, vd. CURTI GIALDINO C., *op. cit.* 226: "[u]na operazione di salvataggio, denominata *Eagle Claw* o *Evening Light*, avviata il 24 aprile 1980, fallì, soprattutto a causa di imprevisti eventi atmosferici, oltre ad uno scarso coordinamento tra le forze in campo, con perdita di vite umane (8 militari statunitensi) e di mezzi (tutti e sei gli elicotteri *Sea Stallion* decollati dalla portaerei *Nimitz* ed un C-130). A seguito del tentativo di salvataggio i 52 ostaggi furono prelevati dall'ambasciata di Teheran e distribuiti in varie località del Paese. Viceversa andò a buon fine l'operazione, organizzata dalla CIA con il pieno appoggio del governo del Canada, (nota come Canadian Caper) di esfiltrazione dall'Iran dei 6 diplomatici che, fuggiti dall'ambasciata assediata, avevano trovato ospitalità nelle residenze di due diplomatici canadesi, attraverso la simulazione della visita in Iran e conseguente partenza, il 28 gennaio 1980, di una *troupe* cinematografica con passaporti canadesi di copertura, in cerca di una appropriata *location* per un presunto *film* di fantascienza, denominato *Argo*."

[166] *Case Concerning Diplomatic and Consular Staff in Teheran*, Order (15 December 1979) ICJ §22.

[167] *Ibidem*.

[168] Vd. CURTI GIALDINO C., *op. cit.* 236.

Central Intelligence Agency sarebbe stata coinvolta persino nel precedente colpo di Stato del 1953, oltre ad aver perpetrato altre (non meglio specificate) attività di spionaggio.[169] Peraltro l'Iran non comparì nel successivo giudizio,[170] precludendosi la possibilità di allegare tali affermazioni e di consentire quindi una pronuncia specificatamente indirizzata al tema dello spionaggio.

La CIG cionondimeno affrontò la questione. Nella successiva sentenza del 24 Maggio 1980, la Corte notò che pure nell'eventualità in cui le accuse iraniane fossero state veritiere, non sarebbero state efficaci avverso le pretese degli USA:

> *[t]he Vienna Conventions of 1961 and 1963 contain express provisions to meet the case when members of an embassy staff, under the cover of diplomatic privileges and immunities, engage in such abuses of their functions as espionage or interference in the interna1 affairs of the receiving State.*[171]

La Corte fa riferimento in questo caso all'Art. 9 della CVRD: il diplomatico colpevole di spionaggio o altre attività clandestine può essere dichiarato *persona non grata*. La Convenzione, infatti, instaura un cd. "*self-contained regime*": se pure una delle parti ha abusato delle immunità o di una qualunque delle previsioni in essa contenute, non sono ammesse limitazioni alla libertà personale o altre misure di tipo ritorsivo.[172] L'unica azione consentita è racchiusa nel medesimo testo normativo ed è per l'appunto nell'Art. 9.[173]

Contro gli abusi più gravi lo Stato accreditatario possiede un mezzo ulteriore, da considerarsi però come *extrema ratio*:

> *[the receiving state] has in its hands a more radical remedy if abuses of their functions by members of a mission reach serious proportions. This is the power which every receiving State has, at its own discretion, to break*

---

[169] S CHESTERMAN, *op. cit.* §8.
[170] Che ebbe comunque luogo ex Art. 53 dello Statuto della CIG.
[171] *Case Concerning Diplomatic and Consular Staff in Tehran* (24 May 1980) ICJ §84.
[172] Cionondimeno, la Corte ammise (in conformità con il commentario ufficiale della ILC alla Convenzione del 1961) che "*[n]aturally, the observance of this principle does not mean – and this the Applicant Government expressly acknowledges – that a diplomatic agent caught in the act of committing an assault or other offence may not, on occasion, be briefly arrested by the police of the receiving State in order to prevent the commission of the particular crime*". Vd. *Case Concerning Diplomatic and Consular Staff in Tehran* (24 May 1980) ICJ §86.
[173] E DENZA, *Diplomatic Law* (Oxford, 3rd edn, 2008) 77.

off diplomatic relations with a sending State and to call for the immediate closure of the offending mission.[174]

In definitiva, la Corte confermò che il comportamento del governo iraniano era stato difforme al diritto internazionale. Lo Stato veniva condannato innanzitutto per non aver adempiuto ai propri obblighi ex Art. 22(2) della Convenzione del 1961.[175] Inoltre, il beneplacito delle autorità nazionali a fronte dell'avvenuta occupazione rendeva i militanti degli agenti *de facto* dello Stato iraniano.[176] Fu riconosciuta la piena responsabilità della Repubblica Islamica per i fatti accaduti ed il governo fu condannato a prendere ogni misura necessaria per il rilascio degli ostaggi e dell'ambasciata nel suo complesso.

In aggiunta ai *findings* della CIG esistono altri mezzi che, secondo il CHESTERMAN, posso aiutare quantomeno ad arginare la raccolta di *intelligence*: l'Art. 11 CVRD (lo Stato accreditatario può limitare le dimensioni e la composizione della missione), gli Artt. 27(1) e 12 (subordinano l'installazione di un posto radiofonico emittente e di uffici regionali all'autorizzazione dello Stato accreditatario), e l'Art. 26 (possibili restrizioni alla libertà di movimento del diplomatico per ragioni di sicurezza nazionale).[177]

Il WARD notava a ragione come il rimedio della *persona non grata* (ma ciò si può estendere agli altri articoli appena elencati) serva solo a neutralizzare temporaneamente l'operazione di spionaggio, senza incidere efficacemente sulla fonte del problema.[178] L'autore auspicava un emendamento, se non anche un

---

[174] *Case Concerning Diplomatic and Consular Staff in Tehran* (24 May 1980) ICJ §85.

[175] "Lo Stato accreditatario è particolarmente tenuto a prendere tutte le misure appropriate per impedire che le stanze della missione siano invase o danneggiate, la pace della missione sia turbata, e la dignità della stessa diminuita"; *cfr.* E DENZA, *op. cit.* 164-165: la prassi dell'Iran era stata ben diversa in casi analoghi. Ad esempio, durante l'assedio dell'ambasciata iraniana a Londra (nel 1980), veniva invocato l'obbligo delle autorità inglesi di difendere la sede diplomatica; *cfr.* CURTI GIALDINO C., *op. cit.* 181: "gli Stati Uniti lamentarono la violazione dell'art. 47 CVRD (e dell'art. 72 CVRC) rilevando che il governo dell'Iran aveva protetto le sedi diplomatiche del Regno Unito e dell'Unione Sovietica e l'ufficio consolare britannico a Kermanshah, che, temporaneamente occupate da gruppi di individui, erano state liberate su ordine dello stesso Ayatollah Komeini."

[176] *Case Concerning Diplomatic and Consular Staff in Tehran* (24 May 1980) ICJ §74: "*[t]he approval given to these facts by the Ayatollah Khomeini and other organs of the Iranian State, and the decision to perpetuate them, translated continuing occupation of the Embassy and the detention of the hostages into acts of that State. The militants, authors of the invasion and jailers of the hostages, had now become agents of the Iranian State for whose acts the State itself was internationally responsible*"; *cfr.* E DENZA, *op. cit.*

[177] Più in generale, l'Art.41 della Convenzione vieta qualsiasi attività incompatibile con le funzioni della missione ed impone il rispetto delle leggi e dei regolamenti dello Stato accreditatario.

[178] N P WARD, *op. cit.* 667.

nuovo trattato, volto a negare le immunità diplomatiche e consolari qualora siano state condotte operazioni di spionaggio. Queste sarebbero incompatibili con le funzioni della missione e con i principi stessi della Convenzione.[179]

Premesso che nel caso di specie ci si riferisce unicamente a diplomatici in carica,[180] la soluzione proposta mostra almeno due limiti evidenti. Innanzitutto, il WARD stesso riconosce che una riforma del diritto vigente in questo senso costituirebbe un'arma a doppio taglio: negare le immunità ai "diplomatici-spia" stranieri, comporta che i propri agenti all'estero ricevano il medesimo trattamento.[181]

La seconda questione riguarda il pericolo insito nell'introduzione di deroghe alle immunità personali. La disciplina delle immunità è finalizzata al sereno esercizio delle funzioni del diplomatico. Prevedere anche solo una eccezione come quella in esame, implica la possibilità di sottoporre l'agente al procedimento penale nello Stato accreditatario. Ciò significherebbe frustrare *tout court* l'effettività delle immunità.[182] Inoltre, nel peggiore dei casi si presta il fianco a comportamenti persecutori da parte degli organi giurisdizionali del paese accreditatario, con la conseguente impossibilità sostanziale di svolgere le funzioni.

Per le medesime ragioni, non è ipotizzabile una sospensione unilaterale delle immunità ad opera dello Stato accreditatario.[183] Se da una parte è condivisibile che la raccolta di *intelligence* segreta da parte del personale diplomatico possa integrare una violazione dell'Articolo 3(1)(d) CVRD,[184] per ciò solo non può essere citato in giudizio personalmente l'agente. La responsabilità, se davvero è stato compiuto un illecito, deve ricadere unicamente sullo Stato accreditante. Quanto detto è confermato dalla *International Law Commission*, che

[179] N P WARD, *op. cit.* 666-667.
[180] Per diplomatici e alte cariche dello Stato cessati dalle funzioni, vd. *supra*.
[181] Peraltro l'autore liquidava il problema confidando nel vantaggio tecnico che gli Stati Uniti detengono, avendo a disposizione diverse agenzie di *intellicence* in grado di operare efficacemente anche al di fuori delle sedi diplomatiche; *cfr.* N P WARD, *op. cit.* 669-670. *Cfr.* le parole discordanti di J RADSAN, *op. cit.* 614: "*lack of a U.S. diplomatic presence in Iran makes recruiting assets there difficult*".
[182] N GRIEF, *op. cit.* 49.
[183] *Ibidem*.
[184] "[I]nformarsi, con ogni mezzo *lecito*, delle condizioni e dell'evoluzione degli avvenimenti nello Stato accreditatario e fare rapporto a tale riguardo allo Stato accreditante" (corsivo aggiunto); *cfr.* il più ampio divieto di cui all'Articolo 41(3).

asserisce: "*[f]ailure by a diplomatic agent to fulfill his obligations does not absolve the receiving State from its duty to respect the agent's immunity.*"[185]

Nei prossimi paragrafi saranno presentati due incidenti internazionali, allo scopo di esplorare alcune situazioni peculiari in cui si è verificato un abuso delle immunità diplomatiche.

3.1. Il caso Kostadinov

Kostadinov era un impiegato statale della Repubblica Popolare di Bulgaria e membro di una missione commerciale a New York.[186] Nel 1983 fu arrestato dalle autorità federali per presunte attività di spionaggio e cospirazione, in forza dello *Espionage Act*.[187] Stando alle registrazioni audiovisive raccolte dall'FBI, Kostadinov aveva offerto una somma di denaro in cambio di documenti segreti del *Department of Energy*.[188] La difesa di Kostadinov consistette nel richiedere l'archiviazione. Asseriva che in qualità di membro del "personale amministrativo e tecnico" dell'ambasciata bulgara, godeva delle immunità diplomatiche ex Art. 37(2) CVRD.[189] Effettivamente, Kostadinov era stato schedato presso il Dipartimento di Stato come "*assistant commercial counselor of the Bulgarian Embassy's commercial counselor's office*".[190] Questa fu la principale ragione per cui la *District Court* in primo grado accolse le richieste di Kostadinov, nonostante le argomentazioni contrarie del Governo.[191] La Corte d'Appello, basandosi soprattutto sui commentari ufficiali della ILC,[192] rovesciò la decisione.[193]

---

[185] ILC, "Commentary to Draft Article 40" (1958) 2 Yearbook of the International Law Commission 90 §1.
[186] B G LARK, "Diplomatic Immunity-Open-Door Policy to Espionage Activity Avoided" (1986) 7 N Y L Sch J Int'l & Comp L 267.
[187] 18 U.S.C. §794(a); 18 U.S.C. §794(c).
[188] B G LARK, *op. cit.* 267.
[189] *Ibidem*, 268.
[190] *Ibidem*, 272-273; vd. CURTI GIALDINO C., *op. cit.* 92: "Il *personale impiegato nel servizio amministrativo e tecnico* della missione (archivi, contabilità, segretariato, traduzione, interpretazione, servizi di comunicazione) non avente funzioni diplomatiche, inviato dallo Stato interessato o assunto sul posto, il *personale di servizio* impiegato nel servizio domestico della missione ed i *domestici privati* (camerieri, cuochi, ecc.) dei membri della missione deve essere soltanto notificato, con nota verbale, al Ministero degli Affari esteri dello Stato ricevente e l'inizio delle relative funzioni non presuppone particolari formalità protocollari (art. 10 CVRD). Tuttavia, anche rispetto a questo tipo di personale, quando esso abbia la cittadinanza dello Stato inviante o di uno Stato terzo, occorre che sussista il consenso dello Stato ricevente".
[191] B G LARK, *op. cit.* 273.
[192] ILC, "Report of International Law Commission to the General Assembly" [1958] 2 Y B Intl'l L Comm 89.

Innanzitutto, la Corte concluse che Kostadinov non poteva essere considerato un membro della "missione" per il solo fatto di aver lavorato nelle stanze della missione. La seconda argomentazione della Corte faceva leva invece sul concetto di *persona non grata* ex Art. 9 della Convenzione. La prassi costante del Governo, in effetti, era sempre stata quella di concedere lo status di diplomatico unicamente ai capi delle missioni commerciali, se situate al di fuori di Washington D.C.[194] Ancora, a Kostadinov non sarebbe stata rilasciata alcuna "carta d'identità diplomatica" dal Dipartimento di Stato.[195] Questi elementi di fatto, che ad una prima lettura possono apparire ambigui o meramente indiziari, sono probabilmente avvalorati dal dettato dell'Art. 4 della Convenzione, che impone allo Stato accreditante l'onere di verificare il gradimento della persona che si intende accreditare.[196] Ciò che solleva seri dubbi, piuttosto, è l'ammissibilità di una dichiarazione tacita di *persona non grata*. Il Dipartimento di Stato, va ricordato, non si era pronunciato né in un senso, né in un altro. È certamente più convincente l'ultima parte della motivazione, fondata sull'Art. 11 della Convenzione:

> 1. Mancando un accordo esplicito circa il numero dei membri del personale della missione, lo Stato accreditatario può esigere che esso sia mantenuto nei limiti che considera ragionevoli e normali, avuto riguardo alle circostanze e condizioni dominanti nello stesso e ai bisogni della missione della quale si tratta.
>
> 2. Negli stessi limiti e senza discriminazione, lo Stato accreditatario può parimente ricusare d'ammettere funzionari d'una determinata categoria.

Questo troverebbe coerente applicazione nella prassi del Governo di accordare le immunità diplomatiche solo ai capi delle missioni, se queste si trovano fuori dell'area di Washington.[197] La formulazione "mancando un accordo esplicito", peraltro, si coniuga molto più facilmente col silenzio del Dipartimento di Stato. In

[193] B G LARK, *op. cit.* 274.
[194] *Ibidem*, 275.
[195] *Ibidem*.
[196] CURTI GIALDINO C., *op. cit.* 82-85.
[197] *Ibidem*, 279.

definitiva, la decisione della Corte d'Appello può considerarsi corretta, ma non accurata nel riferimento all'Art. 9 CVRD.[198]

Il caso in esame mostra che lo Stato accreditatario non è completamente privo di mezzi contro il diplomatico-spia. È innegabile che il diplomatico correttamente accreditato goda dell'immunità dalla giurisdizione civile e penale (con limitatissime eccezioni).[199] Ciò vale tanto per i capi-missione (e.g. Ambasciatori, Ministri plenipotenziari, Incaricati d'Affari) quanto per il personale diplomatico (i.a. ministri, consiglieri, segretari di legazione).[200] Persino ai familiari del diplomatico[201] si estendono i privilegi e le immunità ex Artt. 29-36 VCRD, posto che non siano cittadini dello Stato accreditatario.[202] Come appurato *supra*, il diritto consuetudinario estende le immunità qui descritte pure alle più alte cariche dello Stato (Capo di Stato, di Governo e Ministro degli Affari Esteri). Al contrario, i funzionari consolari non godono di alcuna immunità (neppure civile) per gli atti posti in essere come privati.[203] Ad essi è riconosciuta unicamente l'immunità organica, i.e. per atti compiuti nell'esercizio delle funzioni.[204]

Le regole appena enunciate, si ricorda, sono finalizzate al sereno svolgimento della missione ("*ne impediatur legatio*"). D'altro canto lo Stato offeso, in situazioni che ricalcano l'affare Kostadinov, può riuscire a dimostrare

---

[198] *Ibidem*, 280.
[199] Vd. *supra*.
[200] CONFORTI B., *op. cit.* 262.
[201] Per definire il concetto di "famiglia", vd. CURTI GIALDINO C., *op. cit.* 258: "deve trattarsi di persone «conviventi», cioè che coabitano effettivamente con l'agente diplomatico nella stessa residenza e da lui dipendono economicamente […] Secondo il commentario della CDI, rientrano nel concetto di familiare dell'agente diplomatico o del personale amministrativo e tecnico: *a*) il coniuge, convivente, non separato; *b*) i figli minori (18/21 anni secondo gli ordinamenti), non emancipati, rispetto ai quali l'agente diplomatico esercita la potestà genitoriale, siano essi figli nati dal matrimonio con il coniuge ovvero fuori del matrimonio, ovvero siano figli solo del coniuge, compresi i figli adulterini riconosciuti e gli affidatari; *c*) i figli maggiorenni incapaci, conviventi, dell'agente diplomatico, del coniuge o di entrambi; *d*) i genitori dell'agente diplomatico o del coniuge conviventi e dipendenti dall'agente diplomatico; *e*) i fratelli e sorelle minorenni non emancipati dell'agente diplomatico o del coniuge, conviventi, rispetto ai quali l'agente diplomatico o il coniuge esercitino la potestà genitoriale; *f*) i fratelli o le sorelle maggiorenni ma incapaci, conviventi, dei quali l'agente diplomatico o il coniuge hanno la tutela"; *cfr.* E DENZA, *op. cit.* 393-396.
[202] Art. 37(1) CVRD; *cfr.* CURTI GIALDINO C., *op. cit.* 258-261; vd. *Skeen v. Federative Republic of Brazil* [1983] 566 F Supp 1414 (immunità personale riconosciuta al nipote di un diplomatico brasiliano che, all'uscita di un locale negli Stati Uniti, aveva sparato ad un cittadino americano); CONFORTI B., *op. cit.*
[203] CURTI GIALDINO C., *op. cit.* 411.
[204] RONZITTI N., *op. cit.* 153; CONFORTI B., *op. cit.* 263.

che taluni soggetti non rientrino nella definizione di “personale della missione” o “personale diplomatico”. Così facendo se non altro è possibile arginare una grave falla nella sicurezza nazionale, insanabile a causa della natura cogente delle immunità diplomatiche.

3.2. L’affare Zakharov – Daniloff

Il 23 Agosto 1986 Gennadi F. Zakharov, cittadino sovietico impiegato presso le Nazioni Unite, fu arrestato a New York da agenti federali.[205] Ancora una volta le accuse riguardavano presunte attività di spionaggio.[206] Quasi contemporaneamente a Mosca veniva arrestato per le stesse ragioni Nicholas S. Daniloff, corrispondente di una rivista americana. I due vennero presto rilasciati e presi in custodia dalle rispettive ambasciate.[207] Durante l’amministrazione Reagan, il problema dello spionaggio sovietico era particolarmente sentito. Solo alcuni mesi prima il governo USA aveva demandato una drastica riduzione del personale russo, ucraino e bielorusso presso le Nazioni Unite, proprio per fronteggiare il problema.[208] Considerando congiuntamente la riluttanza del Cremlino a richiamare i propri delegati e l’arresto di Daniloff, si comprende perché il Dipartimento di Stato presentò una lista di venticinque delegati sovietici presso le Nazioni Unite che avrebbero dovuto lasciare il paese entro il 1° Ottobre del medesimo anno. L’URSS richiamò i diplomatici indicati e permise a Daniloff di tornare in patria.[209] Tuttavia, non mancarono ritorsioni. Cinque agenti americani furono espulsi poco tempo dopo da Mosca e Leningrado. A loro volta gli USA espulsero ben cinquantacinque membri del personale consolare e diplomatico allocato tra Washington e San Francisco. Seguì un’ultima ritorsione dell’URSS, che espulse altri cinque diplomatici americani e rimosse parte del personale sovietico presente nell’ambasciata americana.

La vicenda dimostra in modo evidente quanto fosse capillare la diffusione di spie tra i diplomatici (se non anche ambasciatori) di entrambi i blocchi, durante la

[205] N S KHURUSHCHEV, “The "Zakharov-Daniloff Affair," the Diplomatic Expulsions of October 1986, and the Hostile Espionage Threat Facing the United States of America” (1988) 14 Brook J Int'l L 109.
[206] *Ibidem*, 113.
[207] *Ibidem*.
[208] *Ibidem*, 111-112.
[209] *Ibidem*, 114-115.

Guerra Fredda.[210] Ancora, si nota la predilezione per una soluzione stragiudiziale di simili dispute. Da una parte, ciò è reso inevitabile dal regime assoluto delle immunità ed è perfettamente lecito. D'altro canto, un sistema di ritorsioni a catena è poco raccomandabile sul piano delle relazioni internazionali, che ne escono inevitabilmente danneggiate.

Da ultimo, l'affare Zakharov – Daniloff si rivela utile per illustrare il delicato rapporto tra immunità dei cittadini stranieri accreditati presso un'organizzazione internazionale (le Nazioni Unite, in questo caso) e la capacità dello Stato di sede (gli Stati Uniti) di tutelarsi in caso di attività illecite (spionaggio e cospirazione). In linea con la prassi generalmente diffusa, si ritiene che lo Stato ospite non abbia il diritto di dichiarare *persona non grata* i membri del personale di una missione permanente.[211] Di norma lo Stato in questione non è tenuto ad esprimere il proprio gradimento nei confronti di tali soggetti, né viene operato un accreditamento diretto.[212] Gli Stati Uniti, d'altro canto, non si uniformano alla consuetudine internazionale. L'Accordo di sede con l'ONU, nel caso di specie, prevede la possibilità di pretendere il richiamo dei membri delle missioni permanenti "*in accordance with the customary procedure applicable to diplomatic envoys accredited to the United States*".[213] In aggiunta, la Sezione §13 dell'Accordo riconosce allo Stato di sede "*full control and authority over the entry of persons or property into the territory of the United States*".[214] L'orientamento è stato avallato più volte dalla giurisprudenza statunitense, che anzi ravvisa nel testo citato una sorta di veto sull'ammissione dei membri delle missioni permanenti.[215]

---

[210] *Ibidem*, 120.
[211] CURTI GIALDINO C., *op. cit.* 166-167: il principio vale anche nel caso in cui siano state compiute infrazioni gravi.
[212] *Ibidem*; Y L LING, "A Comparative Study of the Privileges and Immunities of United Nations Member Representatives and Officials With the Traditional Privileges and Immunities of Diplomatic Agents" [1976] 33 Wash & Lee L Rev 125, 155; N S KHURUSHCHEV, *op. cit.* 134.
[213] *Agreement Between the United Nations and the United States Regarding the Headquarters of the United Nations, Signed June 26, 1947, and Approved by the General Assembly October 31, 1947*, §15(3); CURTI GIALDINO C., *op. cit.* 167.
[214] *Agreement Between the United Nations and the United States Regarding the Headquarters of the United Nations, Signed June 26, 1947, and Approved by the General Assembly October 31, 1947*, §13(3)(d).
[215] Vd. *United States v. Enger* [1978] 472 F Supp 502; *United States v. Coplon* [1949] 84 F Supp 472ss; *United States ex rel Casanova v. Fitzpatrick* [1963] 214 F Supp 425, 437; CURTI GIALDINO C., *op. cit.* 166.

Bisogna segnalare, infine, che nel caso particolare in cui l'abuso delle immunità porti ad una minaccia per la sicurezza nazionale (e.g. attività terroristiche o di spionaggio) la consuetudine tende ad essere più omogenea.[216] Infatti, la Convenzione del 1947 sui privilegi e le immunità degli Istituti specializzati dell'ONU, nonché la maggior parte degli accordi di sede esistenti, prevedono la possibilità di chiedere il richiamo al fine di preservare l'incolumità dello Stato.[217] *Rectius*, nel caso di violazioni gravi del diritto vigente nello Stato ospite, dovrebbe essere lo Stato di invio a disporre il richiamo immediato (oppure a rinunciare all'immunità del proprio agente).[218] La Convenzione di Vienna del 1975 sulla rappresentanza degli Stati presso le organizzazioni internazionali a vocazione universale a tal proposito prescrive che:

> in caso di infrazione grave e manifesta della legislazione penale dello Stato ospite da parte di una persona che beneficia dell'immunità di giurisdizione, lo Stato di invio, a meno che non rinunci all'immunità, richiama la persona in questione, pone fine alla funzione che la persona esercita presso la missione, la delegazione o la missione di osservazione, o ne assicura la partenza, secondo il caso. Lo Stato d'invio si comporta nello stesso modo in caso di ingerenza grave e manifesta negli affari interni dello Stato ospite. Le disposizioni di questo paragrafo non si applicano nel caso di un atto compiuto nell'esercizio delle funzioni della missione o nello svolgimento di compiti della delegazione.[219]

4. Violazione di sedi diplomatiche

Il quadro giuridico è più lineare nella diversa situazione in cui il diplomatico non sia la spia ma lo spiato. L'Art. 22 della Convenzione di Vienna contiene una norma essenziale nelle relazioni diplomatiche, concernente l'inviolabilità delle stanze della missione.[220] In particolare, i primi due paragrafi indicano che:

---

[216] CURTI GIALDINO C., *op. cit.*
[217] *Ibidem*; *cfr.* Accordo di Sede fra l'Italia e la FAO del 31 Ottobre 1950.
[218] CURTI GIALDINO C., *op. cit.*
[219] CRSOI, Art. 77(2).
[220] CURTI GIALDINO C., *op. cit.* 190-191.

> 1. Le stanze della missione sono inviolabili. Senza il consenso del capomissione, è vietato agli agenti dello Stato accreditatario accedere alle stesse.
>
> 2. Lo Stato accreditatario è particolarmente tenuto a prendere tutte le misure appropriate per impedire che le stanze della missione siano invase o danneggiate, la pace della missione sia turbata, e la dignità della stessa diminuita.

L'obbligo imposto allo Stato accreditatario dunque non è solo di astensione, ma anche di adoperarsi affinché sia garantita la "pace della missione".[221] La regola è perentoria, tanto più che ogni suggerimento di inserire nel testo eccezioni operanti in caso di emergenza, è stato stroncato dalla ILC.[222]

Allo stesso modo sono inviolabili gli archivi della missione "in ogni tempo e ovunque si trovino",[223] così come la dimora privata, i documenti e la corrispondenza dell'agente.[224] Una limitatissima deroga riguarda solo i suoi beni personali, che sono esecutabili ex Art. 31(1)(a) e (c).[225]

Il tema dell'inviolabilità delle sedi diplomatiche torna in auge in tempi recentissimi, in considerazione delle rivelazioni fatte da Edward Snowden. Assumendo che le informazioni svelate siano veritiere, sarebbero state spiate una quantità notevole di ambasciate e missioni diplomatiche negli USA (la stampa oscilla tra le 38 e le 80). A prescindere dal numero effettivo, la violazione dell'Art. 22 sarebbe palese.[226] Si è di fronte ad una situazione in cui l'operazione di *intelligence*, dunque, costituisce pacificamente un illecito internazionale.

Il "Progetto di Articoli sulla Responsabilità dello Stato"[227] prevede come prima conseguenza l'insorgenza di un obbligo di cessazione e non ripetizione

---

[221] Contraddicendo solo in parte quanto detto *supra*, più volte nella pratica le truppe dello Stato accreditatario si sono introdotte in sedi diplomatiche al fine di adempiere il proprio obbligo di protezione (es. per impedire atti di terrorismo). Si ritiene comunque necessaria l'autorizzazione dello Stato accreditante; H P HESTERMEYER, "Vienna Convention and Diplomatic Relations (1961)" [2009] Max Planck Encyclopedia of Public International Law §3(25): http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1004?rskey=TXLvwj&result=2&prd=EPIL.

[222] H P HESTERMEYER, *op. cit.*

[223] Art. 30(1) della Convenzione

[224] Art. 24 della Convenzione.

[225] Art. 30(2) della Convenzione.

[226] RONZITTI N., *op. cit.*

[227] Progetto di Articoli sulla Responsabilità dello Stato della Commissione del Diritto Internazionale (2001), comunemente considerato essere ricognitivo del diritto consuetudinario.

dell'atto illecito.[228] Inoltre, lo Stato offensore ha l'obbligo di riparare integralmente il pregiudizio causato.[229]

Tra le forme di riparazione applicabili,[230] nel caso di specie, possono ipotizzarsi il risarcimento del danno[231] o (più realisticamente, vista la natura immateriale dell'illecito) una qualche forma di soddisfazione. Un esempio può essere quello di una presentazione ufficiale di scuse da parte del governo americano.[232] Nel suo discorso tenutosi il 17 Gennaio 2014, effettivamente, il presidente Obama ha dichiarato di voler porre fine alla sorveglianza sugli alleati. Se dunque c'è stata una *pars destruens* in cui gli USA hanno ammesso l'esistenza di un illecito, ancora non può parlarsi di "soddisfazione" data l'assenza di scuse concrete per gli atti pregressi. Al contrario, lo scontro diplomatico con i paesi spiati è ancora acceso.

Allo stato attuale, esistono i presupposti per attivare i mezzi di risoluzione delle controversie previsti dal Protocollo Facoltativo alla Convenzione di Vienna del 1961.[233] *Rectius*, con ogni probabilità è attivabile il solo ricorso di fronte alla Corte Internazionale di Giustizia di cui all'Art. 1. Infatti, per l'attivazione di una procedura arbitrale[234] o di conciliazione,[235] ormai dovrebbe essere scaduto per tutti i paesi offesi il termine di due mesi previsto a pena di decadenza. Fra i paesi firmatari del Protocollo figurano molti degli Stati interessati. Tra questi spiccano gli Stati Uniti e la Germania,[236] principali attori del dibattito odierno su *privacy* e libertà.

Infine, pare che l'attività di sorveglianza perpetrata dall'NSA non si sia limitata alle ambasciate, ma abbia coinvolto anche diverse organizzazioni internazionali. In questo caso, la disciplina è del tutto analoga a quella dettata dalla Convenzione di Vienna, con un appunto: occorre sempre tenere in

---

[228] *Ibidem*, Art. 30.
[229] *Ibidem*, Art. 31(1).
[230] *Ibidem*, Artt. 34-39.
[231] *Ibidem*, Art. 36.
[232] *Ibidem*, Art. 37(2); CONFORTI B., *op. cit.* 409.
[233] Protocollo di Firma Facoltativa alla Convenzione di Vienna sulle Relazioni Diplomatiche del 1961; RONZITTI N., *op. cit.*
[234] Protocollo di Firma Facoltativa, Art. 2.
[235] *Ibidem*, Art. 3.
[236] Per i quali il Protocollo è entrato in vigore, rispettivamente, il 13 Dicembre 1972 e l'11 Novembre 1964.

considerazione l'accordo di sede con lo Stato ospite.[237] Prendendo ad esempio le Nazioni Unite, sono due le norme rilevanti. L'*Headquarters Agreement*[238] tra ONU e Stati Uniti stabilisce che:

> *[t]he headquarters district shall be inviolable. Federal, state or local officers or officials of the United States, whether administrative, judicial, military or police, shall not enter the headquarters district to perform any official duties therein except with the consent of and under conditions agreed to by the Secretary-General. The service of legal process, including the seizure of private property, may take place within the headquarters district only with the consent of and under conditions approved by the Secretary-General.*[239]

Ancora, la *Convention on the Privileges and Immunities of the United Nations* del 1946 prevede che:

> *The premises of the United Nations shall be inviolable. The property and assets of the United Nations, wherever located and by whomsoever held, shall be immune from search, requisition, confiscation, expropriation and any other form of interference, whether by executive, administrative, judicial or legislative action.*[240]

La Sezione quarta del medesimo Articolo, completa la regolamentazione in esame statuendo che:

> *The archives of the United Nations, and in general all documents belonging to it or held by it, shall be inviolable wherever located.*

Come è facile intuire, si tratta di norme speculari a quelle presenti nella Convenzione di Vienna, esaminate nel presente paragrafo. L'unica differenza sostanziale può riscontrarsi nell'impossibilità di attivare il ricorso di fronte alla Corte Internazionale, dal momento che le organizzazioni internazionali non detengono il cd. *locus standi judiciis*.[241]

---

[237] RONZITTI N., *op. cit.*
[238] *Agreement Between the United Nations and the United States Regarding the Headquarters of the United Nations, Signed June 26, 1947, and Approved by the General Assembly October 31, 1947*.
[239] *Ibidem*, §6(a).
[240] *Convention on the Privileges and Immunities of the United Nations* del 1946, Art. 2§3.
[241] Statuto della Corte Internazionale di Giustizia del 26 giugno 1945, Art. 34(1).

5. Sviluppi recenti nel diritto internazionale: *bulk data collection*

Già in diverse occasioni si è anticipato che lo scandalo conosciuto come *datagate* ha scosso profondamente l'opinione pubblica, portando finalmente i governi nazionali ad affrontare l'ambigua materia dell'*intelligence gathering* in tempo di pace. Rinviando al capitolo successivo per una trattazione approfondita, il presente paragrafo si prefigge di sintetizzare le ripercussioni che l'affare Snowden ha avuto sull'*opinio juris* internazionale odierna.

5.1. Provvedimenti in seno all'ONU

Il 18 Dicembre 2013, l'Assemblea Generale ha adottato la Risoluzione A/RES/68/167. Intitolata "*Right to Privacy in the Digital Age*", è stata presentata da Germania e Brasile, due tra i paesi più colpiti dalle agenzie statunitensi. In apertura, la Risoluzione richiama principi ben consolidati in tema di *privacy*. Questi sono racchiusi nella Dichiarazione Universale dei Diritti dell'Uomo e nei due Patti Internazionali del 1966. A seguire, viene condannata ogni condotta lesiva di quegli stessi diritti, inviolabili tanto *online* quanto *offline*. Gli Stati sono chiamati ad interrompere qualsiasi violazione ancora in atto e ad adottare normative efficaci per impedirne di nuove. In particolare si fa appello ai legislatori nazionali per contrastare fenomeni di sorveglianza di massa ed intercettazioni illecite.

Nonostante la Risoluzione sia stata redatta nella forma della dichiarazione di principi, dalla discussione[242] che ha seguito la prima *draft resolution*[243] si evince chiaramente che il reale destinatario sono gli Stati Uniti. Il delegato della Corea del Nord, dichiarando di schierarsi a favore della Risoluzione, tacciava duramente di ipocrisia gli USA, chiedendo la cessazione immediata delle sue operazioni di spionaggio.[244] Così l'Indonesia, con toni più pacati ma comunque decisi, denunciava le recenti pratiche di sorveglianza extraterritoriale in quanto lesive del diritto alla *privacy*. Lo stesso faceva la delegazione del Canada, che pure rientra

[242] A/C.3/68/SR.51.
[243] A/C.3/68/L45/Rev.1.
[244] A/C.3/68/SR.51 §40.

tra i c.d. "*5-eyes*",[245] vale a dire uno dei principali paesi offensori. In effetti, nessuno degli "Stati spioni" si è opposto alla Risoluzione, la quale è stata adottata per *consensus*.[246]

Un altro contributo rilevante apportato dalla Risoluzione è nella procedura di "*follow-up*" di cui alla quinta *operative clause*. Con questa, si chiedeva all'Alto Commissario delle Nazioni Unite per i diritti umani di redigere un rapporto riguardante il diritto alla *privacy* in relazione alla sorveglianza domestica ed extraterritoriale, all'intercettazione delle comunicazioni, alla raccolta massiva di dati. Posto che il contenuto del rapporto sarà oggetto di studio *infra*, in questa sede si può affermare che l'Alto Commissario non ha fatto altro che confermare la posizione comunemente accolta. Nel contemperamento fra esigenze di sicurezza nazionale e diritto alla *privacy* (nonché tutti gli altri diritti umani connessi), quest'ultimo soccombe solo in casi eccezionali, secondo modalità previste dalla legge ed implementate in modo non arbitrario.[247]

Se ancora è presto per parlare di una normativa internazionale in materia di *intelligence*, certamente si assiste alla volontà nuova di porre dei limiti al fenomeno. La dottrina tradizionale, già poco convincente nel relegare *intelligence* e spionaggio al diritto interno, deve essere rivisitata. Lo scenario attuale mostra una situazione ben diversa. Se ci si sofferma unicamente sulla questione del diritto alla *privacy* nell'era digitale, pare in effetti che l'anello debole della legislazione attuale siano i parlamenti nazionali, non il diritto internazionale. Tanto le convenzioni quanto la consuetudine hanno costruito un quadro "chiaro e universale"[248] per la promozione e la protezione del diritto alla *privacy*. La regolamentazione della sorveglianza su larga scala e di fenomeni analoghi, invece, è carente in molti Stati o si dimostra debole conto gli autoritarismi dell'esecutivo. Ciò che si auspica è la prosecuzione dei lavori dell'Assemblea Generale, così da poter consolidare una nuova e soprattutto unitaria *opinio juris* che possa se non altro persuadere la comunità internazionale ad adeguarsi a standard che, a conti fatti, già esistono da tempo.

---

[245] RONZITTI N., *L'ONU Batte un Colpo su Privacy e Spioni* in IAI Rivista Online, 2013: http://www.affarinternazionali.it/articolo.asp?ID=2478.
[246] *Ibidem*; *cfr.* A/C.3/68/SR.51 §§43, 45, 47, 48.
[247] A/HRC/27/37.
[248] *Ibidem*.

5.2. *Privacy* e dati personali in Europa

L'affare Snowden ha colpito con particolare durezza il vecchio continente. I motivi sono molteplici, dal rapporto di fiducia reciproca che perdura (*rectius* perdurava) da decenni tra Stati Uniti ed Europa, al fatto che larga parte dei paesi UE sono al tempo stesso membri NATO. È emersa una verità scomoda, in realtà già nota,[249] ma ammessa con riluttanza: neanche le potenze alleate sono risparmiate dall'attività di *intelligence* in tempo di pace.

Sicuramente il fattore politico non è irrilevante, in questa nuova levata di scudi contro il "cyberspionaggio". Germania e Brasile, paesi i cui premier sono stati sottoposti a sorveglianza diretta dei telefoni cellulari, non a caso sono i principali promotori dei lavori in seno all'ONU di cui si è parlato *supra*. E così l'UE, sempre guidata dal Cancelliere Merkel, si erge a baluardo dei diritti umani alla *privacy* e alla tutela dei dati personali. Gli studiosi[250] riconoscono nella situazione attuale una spaccatura profonda tra le due culture giuridiche, americana ed europea.

Da una parte, gli USA riconoscono nel Quarto Emendamento alla Costituzione l'inviolabilità del diritto alla *privacy* avverso l'irragionevole interferenza del potere esecutivo.[251] Dal punto di vista sostanziale, però, si assiste negli anni ad una progressiva erosione delle libertà civili a vantaggio della sicurezza nazionale. Gli avvenimenti dell'11 Settembre 2001 non fanno che esasperare questa tendenza, consolidando definitivamente una politica di statuti emergenziali ed ampliando in modo virtualmente incontrollabile i poteri dell'esecutivo.

Oltreoceano, l'Europa ha sempre riconosciuto il diritto alla *privacy*, tanto sotto l'egida del Consiglio d'Europa che in ambito UE. Gli strumenti normativi

---

[249] European Parliament – Committee on Civil Liberties, Justice and Home Affairs, "Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs" (2013/2188(INI)); RONZITTI N., *Il Caso Snowden e le Regole dello Spionaggio* in IAI Rivista Online, 2013: http://www.affarinternazionali.it/articolo.asp?ID=2369.

[250] Vd i.a. NINO M., *Il caso* Datagate*: problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy* in 7 Diritti Umani e Diritto Internazionale, 2013, 727.

[251] "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*"

sono molteplici, tutti espressivi di diritti comuni: l'Art. 8 della CEDU, la Convenzione 108/1981, la Direttiva 95/46/CE, l'Art. 16 TFUE e ancora gli Artt. 7 e 8 della Carta di Nizza sono solo i principali. Contrariamente a quanto si può riscontrare negli USA, tutte le disposizioni appena nominate sono sempre state interpretate nel senso di anteporre le libertà civili dell'individuo. Deroghe motivate da esigenze di sicurezza nazionale, devono essere eccezionali e regolate da specifiche previsioni di legge.

Sul piano dell'effettività, però, l'Europa sconta l'instabilità del sistema statunitense. Nell'era digitale, inevitabilmente, anche i cittadini dell'Unione sono sottoposti alla *bulk data collection* delle agenzie federali. Dal rapporto stilato dalla commissione LIBE del Parlamento Europeo,[252] si evince che l'attuale divario negli standard di protezione non è più politicamente né giuridicamente accettabile. La speranza è che proseguano fruttuosamente i lavori sul c.d. "*Umbrella Agreement*", un accordo bilaterale USA-UE finalizzato alla regolamentazione dei trasferimenti di dati tra i due continenti.

6. Lo spionaggio economico

L'ultima forma di *intelligence* che si vuole esaminare è il c.d. spionaggio economico.[253] Il fenomeno, secondo la ricostruzione di ERDOGAN, è cresciuto esponenzialmente al termine della Guerra Fredda.[254] In particolar modo, la proliferazione di sistemi globali di comunicazione ed informazione (i.a. Internet) ne ha facilitato notevolmente la diffusione.[255] Il CHESTERMAN fornisce la seguente definizione di spionaggio economico: "*the use of intelligence capacities for economic rather than national security purposes*".[256] Si evincono

[252] European Parliament – Committee on Civil Liberties, Justice and Home Affairs, Report (2013/2188(INI)).
[253] Noto anche come "spionaggio industriale" o "spionaggio societario".
[254] I ERDOGAN, "Economic Espionage as a New Form of War in the Post Cold-War Period" [2009] 2 USAK Yearbook 267.
[255] *Ibidem*, 269.
[256] Per altre definizioni vd.: "Espionage and Foreign Interference" *Canadian Security Intelligence Service*, http://www.csis.gc.calprrts/spng/index-eng.asp: "*illegal, clandestine or coercive activity by foreign governments in order to gain unauthorized access to economic intelligence, such as proprietary information or technology*"; G E TURNER, "The Threat of Foreign Economic Espionage to U.S. Corporations" [1992] 102d Cong, 2nd Sess., 192 p5: "*surreptitious acquisition of corporate trade secrets, advanced technology, product information, business plans, and various*

immediatamente due caratteri portanti. *In primis,* nonostante la nomenclatura comunemente diffusa, lo "spionaggio" economico può essere esercitato genericamente attraverso una qualsiasi altra delle forme di *intelligence* fin qui menzionate (soprattutto la SIGINT). In secondo luogo, l'oggetto dello spionaggio economico è diverso da quello dello spionaggio "classico". Consiste essenzialmente nel carpire informazioni concernenti la proprietà intellettuale, brevetti o nuovi sviluppi in ambito industriale ed informatico.[257]

La pratica è estremamente diffusa, e non solo tra i paesi economicamente più sviluppati. Pare che i principali attori siano i Paesi asiatici in via di sviluppo, subito seguiti da quelli dell'Europa occidentale.[258] In modo peculiare, se è pur vero che si ha solo di recente la conferma che i paesi alleati non sono risparmiati dall'attività di *intelligence* in tempo di pace, è noto da tempo che "*[i]n the world of economic espionage, there are no true friendly relations*".[259] Si hanno ripercussioni notevoli sugli Stati coinvolti. Le conseguenze primarie sono i danni economici sofferti dalle imprese colpite (anche nell'ordine di miliardi di dollari) e la perdita, comunque ingente, di posti di lavoro.[260]

A questo punto, occorre specificare la posizione del diritto internazionale in merito allo spionaggio economico e quali siano i profili di responsabilità dello Stato offensore. È doveroso premettere che il CHESTERMAN, fra tutti, dubita che si possa realmente distinguere lo spionaggio economico da quello "tradizionale".[261] L'affermazione può essere condivisibile, ma sono necessarie delle specificazioni. Se l'attività di spionaggio economico è condotta da imprese private (e nel solo interesse di imprese private) non può esistere responsabilità internazionale per l'offensore, data la mancanza di capacità giuridica internazionale. Del resto, questo sarà sottoposto alla giurisdizione civile o penale dello Stato offeso.

Se con "spionaggio" si intende invece l'intrusione di un agente dello Stato offensore nel territorio dello Stato offeso (es. al fine di sottrarre segreti industriali),

---

types of proprietary information which can provide competitors with a distinct market advantage."; I ERDOGAN, *op. cit.* 267; *cfr.* C D BAKER, *op. cit.* 1091, 1093.
[257] I ERDOGAN, *op. cit.* 273.
[258] I ERDOGAN, *op. cit.* 279-280; K SEPURA, "Economic Espionage: The Front Line of a New World Economic War" [1998-1999] 26 Syracuse J Int'l L & Com 131.
[259] K SEPURA, *op. cit.* 132.
[260] *Ibidem*, 138.
[261] S CHESTERMAN, *op. cit.*

nulla quaestio. In varie occasioni si è spiegato che una simile condotta costituisce una violazione della sovranità territoriale dello Stato offeso, nonché un illecito internazionale.

Se invece il termine "spionaggio" è usato in senso lato (ad esempio ricomprendendo anche un attacco informatico o l'impiego di cimici), il quadro è più complesso. Sicuramente non può parlarsi di violazione della sovranità territoriale, perché un'intrusione fisica non c'è. Eppure, questo tipo di attività può avere delle ripercussioni sul dominio riservato degli Stati se si pensa che può arrivare ad incidere sul PIL dei Paesi più colpiti.[262] Si potrebbe allora pensare ad una violazione dei principi della già menzionata Risoluzione 2625(XXV), la quale specifica che:

> "*[n]o State may use or encourage the use of* economic, *political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind.*" (Enfasi aggiunta).

Ovviamente, questa ipotesi è plausibile solo se seguita con la dovuta cautela, impiegando un approccio "caso per caso". Riscontrare una violazione della Risoluzione in esame a seguito di un singolo furto di brevetti sarebbe assurdo. Eppure, una condotta reiterata e sistematica ai danni della produzione nazionale di un altro Paese potrebbe coniugarsi con la tesi proposta.[263] Analogamente, sono state richiamate dalla dottrina[264] le Risoluzioni 1236(XII)[265] e 2131(XX)[266] dell'Assemblea Generale delle Nazioni Unite. Queste richiamano rispettivamente i principi di buon vicinato e non ingerenza nelle questioni interne degli Stati, nei quali è stato ravvisato un riferimento indiretto allo spionaggio economico.[267]

A latere delle considerazioni appena fatte, non si può ignorare la normativa esistente in materia di proprietà industriale, spesso volta a condannare furti e pratiche scorrette. La Convenzione di Parigi per la Protezione della Proprietà

---

[262] FAINI M., *op. cit.* 80.
[263] FAINI M., *op. cit.* 77ss.
[264] K SEPURA, *op. cit.* 144-145.
[265] "*Peaceful and Neighbourly Relations Among States*".
[266] "*No State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any State. Consequently, armed intervention* and all other forms *of interference or attempted threats against the personality of the State or against its political,* economic *and cultural elements, are condemned.*" (Enfasi aggiunta).
[267] K SEPURA, *op. cit.* 145.

Industriale del 1967, prima fra tutte, impone agli Stati membri il rispetto dei diritti concernenti la proprietà industriale. Istituisce inoltre un'Unione che, impiegando un'articolata struttura amministrativa,[268] ha lo scopo di assicurare l'effettiva applicazione della Convenzione. La reale efficacia di questo strumento, però, è limitata. La causa, secondo la dottrina, è da ricondursi alla mancanza di norme specificatamente indirizzate allo spionaggio.[269] Altre norme di rilievo sono contenute nell'accordo TRIPs,[270] esito di quello stesso *Urguay Round* che diede vita alla WTO.[271] In particolare l'Art. 39 richiama proprio l'Art. 10*bis* della Convenzione di Parigi, imponendo agli Stati membri il rispetto e la protezione delle informazioni segrete.[272] La forza dell'accordo TRIPs sta nella predisposizione di diversi mezzi di risoluzione delle controversie. Questi prendono la forma di ingiunzioni e procedure per il risarcimento del danno,[273] nonché di misure provvisorie volte ad inibire il comportamento lesivo.[274] Ciononostante, anche l'Accordo si è rivelato col tempo un deterrente debole, forse

[268] Assemblea ex Art. 13, Comitato Esecutivo ex Art. 14, Ufficio Internazionale ex Art. 15; *cfr*. K SEPURA, *op. cit.* 143.

[269] L'unica norma assimilabile, se interpretata estensivamente, sarebbe l'Art. 10*bis* (Concorrenza Sleale):
"1) I paesi dell'Unione sono tenuti ad assicurare ai cittadini dei paesi della Unione una protezione effettiva contro la concorrenza sleale.
2) Costituisce un atto di concorrenza sleale ogni atto di concorrenza contrario agli usi onesti in materia industriale o commerciale […]"; K SEPURA, *op. cit.* 143.

[270] "*Trade-Related Aspects of Intellectual Property Rights*"; vd. S CHESTERMAN, *op. cit.*

[271] K SEPURA, *op. cit.* 143.

[272] "1. Nell'assicurare un'efficace protezione contro la concorrenza sleale ai sensi dell'art. 10-bis della Convenzione di Parigi (1967), i Membri assicurano la protezione delle informazioni segrete conformemente al paragrafo 2 e quella dei dati forniti alle autorità pubbliche o agli organismi pubblici conformemente al paragrafo 3.
2. Le persone fisiche e giuridiche hanno la facoltà di vietare che, salvo proprio consenso, le informazioni sottoposte al loro legittimo controllo siano rivelate a terzi oppure acquisite o utilizzate da parte di terzi in un modo contrario a leali pratiche commerciali nella misura in cui tali informazioni:
a) siano segrete nel senso che non sono, nel loro insieme o nella precisa configurazione e combinazione dei loro elementi, generalmente note o facilmente accessibili a persone che normalmente si occupano del tipo di informazioni in questione;
b) abbiano valore commerciale in quanto segrete; e
c) siano state sottoposte, da parte della persona al cui legittimo controllo sono soggette, a misure adeguate nel caso in questione intesa a mantenerle segrete.
3. I Membri, qualora subordinino l'autorizzazione della commercializzazione di prodotti chimici farmaceutici o agricoli implicanti l'uso di nuove sostanze chimiche alla presentazione di dati relativi a prove o di altri dati segreti, la cui elaborazione comporti un considerevole impegno, assicurano la tutela di tali dati da sleali usi commerciali. Essi inoltre proteggono detti dati dalla divulgazione, salvo nei casi in cui risulti necessaria per proteggere il pubblico o a meno che non vengano prese misure atte a garantire la protezione dei dati contro sleali usi commerciali."

[273] *Agreement on Trade-Related Aspects of Intellectual Property Rights* Artt. 42-49.

[274] *Ibidem*, Art. 50.

sempre per la mancanza di una disposizione specifica contro lo spionaggio industriale.[275]

Si vuole da ultimo affrontare una situazione particolare di spionaggio economico, almeno sul versante soggettivo. *Quid juris* se l'agenzia (pubblica) di *intelligence* che porta a termine l'operazione agisce per conto di un'impresa privata? Ci si riferisce in particolar modo alle rivelazioni secondo le quali la NSA sarebbe stata implicata anche nello spionaggio industriale per conto di imprese private statunitensi. In questo caso, sembra potersi invocare l'Art. 7 del Progetto di Articoli sulla Responsabilità degli Stati:

> Il comportamento di un organo di uno Stato o di una persona o di un ente abilitati ad esercitare prerogative dell'autorità di governo sarà considerato come un atto dello Stato ai sensi del diritto internazionale, se quell'organo, persona o ente agisce in tale qualità, anche se eccede la propria competenza o contravviene ad istruzioni.[276]

In buona sostanza, quando ad agire è un organo pubblico, la responsabilità per l'illecito compiuto viene fatta ricadere sullo Stato a prescindere da ogni considerazione sul controllo effettivo.

7. Attività di *intelligence* e libertà d'espressione

Come esposto nei paragrafi introduttivi della presente trattazione, *intelligence* e spionaggio sono essenzialmente intrisi di clandestinità e segretezza. Formalmente però, le relative operazioni vengono condotte da agenzie governative istituite ai sensi di legge, nel rispetto dell'ordinamento giuridico costituito. Inserendo l'*intelligence* nel gioco democratico dello Stato di diritto, è naturale che la società civile pretenda una trasparenza ed una capacità di controllo che è difficile coniugare con le prerogative di questo tipo di agenzie.[277]

---

[275] K SEPURA, *op. cit.* 144.

[276] *Cfr. Francisco Mallén (United Mexican States) v. U.S.A.* [1927] 4 Reports of International Arbitral Awards 173-190.

[277] "*Democracy depends on the knowledge of people*": T BAKKEN, "The Prosecution of Newspapers, Reporters, and Sources for Disclosing Classified Information: The Government's Softening of The First Amendment" [2013] 45 U Tol L Rev 2.

Ne consegue una consistente pratica di *disclosure*, pubblicazione di informazioni classificate, ad opera dei media.[278] Spesso la fonte di queste notizie "trapelate" sono impiegati pubblici che, pur privi delle autorizzazioni necessarie, rivelano operazioni moralmente se non anche giuridicamente riprovevoli.

Si delinea un attrito profondo tra due valori giuridici di pari dignità: la sicurezza nazionale da una parte e, dall'altra, la libertà d'espressione. L'*affaire* Snowden ne è la manifestazione più recente e macroscopica: rivelare l'esistenza del programma PRISM può essere considerato un gesto nobile dal cittadino che non vuole vedere sacrificato il proprio diritto alla *privacy*, ma gli effetti collaterali possono essere seri. Ad esempio, esiste la concreta possibilità di aver messo in allarme le organizzazioni terroristiche internazionali che usufruivano dei canali di comunicazione monitorati.[279]

A seguire, verrà analizzato l'approccio del legislatore statunitense al problema con riguardo alle rivelazioni del sito *Wikileaks* e dell'ex-collaboratore NSA, Edward Snowden. Seguirà poi un raffronto con i principi tracciati a livello europeo, per evidenziarne le profonde differenze.

7.1. Lo *Espionage Act* e WikiLeaks

Lo *Espionage Act* del 1917[280] è il testo di riferimento negli USA per quanto concerne i crimini relativi allo spionaggio. La Sezione 798(a) recita:

> *Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information […] [s]hall be fined under this title or imprisoned not more than ten years, or both.*

---

[278] Consiglio d'Europa, Assemblea Parlamentare, Comitato per gli Affari Giuridici e i Diritti dell'Uomo, "National security and Access to Information" [24 Giugno 2013] 5 §9; nella letteratura statunitense si parla di *leaks*, essenziali per lo stesso Congresso che difficilmente riesce a controllare in modo effettivo le attività condotte in segreto dall'esecutivo: M PAPANDREA, "Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment" [2014] 94 B U L Rev 468.

[279] Sull'importanza della segretezza nel ramo esecutivo, vd. *United States v Curtiss-Wright Exp Corp* [1936] 299 U.S. 304, 320; M PAPANDREA, *op. cit.* 464.

[280] 18 U.S.C. §§ 792-799.

Essenzialmente viene perseguita, con una formula volutamente ampia, la trasmissione o pubblicazione di informazioni classificate. [281]

Per restringere il campo d'applicazione della norma, un primo passo logico potrebbe essere quello di definire con chiarezza cosa si intende con "informazione classificata". La risposta è contenuta nello *Executive Order* No.13526 del 2009:[282] è "classificata" l'informazione alla quale un impiegato federale abbia attribuito una classificazione.[283] Questa si esprime attraverso tre diciture notorie: *top secret*, *secret* o *confidential*.[284] Fallisce così il primo tentativo di raffinare la portata dello *Espionage Act* §798(a), dal momento che anche questa definizione appare tautologica e subordinata al potere discrezionale dell'organo esecutivo.

Se si ricorre ad un approccio *ratione materiae* (vale a dire sulla base dell'oggetto della classificazione), il risultato non è più incoraggiante. Sul piano prettamente teorico, lo *Executive Order* prescrive la classificazione di qualunque informazione afferente la sicurezza nazionale. [285] Nella pratica, però, non si fornisce una definizione esaustiva di "sicurezza nazionale", se non nel fatto che questa corrisponde alla "*national defense of foreign relations of the United States*".[286] Neanche il concetto di *national defense* gode di maggior chiarezza. La stessa Corte Suprema degli Stati Uniti, nel caso *Gorin,*[287] avallò le conclusioni dello *U.S. Attorney* secondo cui: "*national defense […] is a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness.*"[288]Ammettere che una norma penale si fondi su di un concetto dal significato così deliberatamente vago comporta quantomeno perplessità sulla certezza del diritto, se non anche dubbi di costituzionalità.[289] Il primo emendamento alla costituzione americana, infatti, è adamantino nello statuire che:

---

[281] T BAKKEN, *op. cit.* 4.
[282] *Executive Order* No.13526 – *Classified National Security Information* del 29 Dicembre 2009: "*This order prescribes a uniform system for classifying, safeguarding and declassifying national security information, including information relating to defense against transnational terrorism*"; T BAKKEN, *op. cit.* 2.
[283] *Executive Order* No.13526, 75 Fed Reg 726 (Dec 29, 2009); T BAKKEN, *op. cit.* 4.
[284] T BAKKEN, *op. cit.* 2.
[285] *Ibidem*; M PAPANDREA, *op. cit.* 475.
[286] *Executive Order* No.13526, 75 Fed Reg 707, 729; T BAKKEN, *op. cit.* 4.
[287] *Gorin v United States* [1941] 312 U.S. 19.
[288] *Gorin v United States* [1941] 312 U.S. 28; T BAKKEN, *op. cit.* 5.
[289] T BAKKEN, *op. cit.* 3, 4.

[c]ongress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press*; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances* (enfasi aggiunta).

A fronte di ciò, il governo degli Stati Uniti era sempre stato molto cauto nel perseguire reporter o giornali per aver "semplicemente" ricevuto informazioni classificate.[290] In tempi recenti si assiste ad un notevole cambiamento di rotta nei confronti del sito *WikiLeaks*,[291] la nota "banca delle informazioni" che in più di un'occasione si è rivelata una spina nel fianco della politica estera USA. Secondo quanto riportato sul sito stesso,[292] pare che il fondatore Julian Assange sia stato incriminato in segreto dal governo federale (in forza dello *Espionage Act*) per aver pubblicato informazioni ricevute dal soldato semplice Bradley Manning.[293] Prescindendo dalle questioni di costituzionalità relative ad un *secret indictment*, ciò su cui si vuole porre l'accento è la circostanza che Assange in questo frangente era unicamente destinatario ("*recipient*") e non anche colui che in prima battuta aveva sottratto o distribuito l'informazione secretata.[294] Questa particolare situazione non ha precedenti neanche nell'esperienza del governo statunitense, che in casi analoghi preferiva sempre cercare di ottenere la rivelazione della fonte, emettendo un mandato di comparizione ("*subpoena*") nei confronti del reporter.[295]

Riassumendo, se l'incriminazione di Assange fosse confermata, si creerebbe un precedente per cui anche il reporter è punibile come spia per la pubblicazione di informazioni classificate ottenute *legalmente*.[296]

---

[290] *Ibidem*, 7; J L HESTER, "The Espionage Act and Today's High-Tech Terrorist" (2010-2011) 12 N C J L & Tech 190; M PAPANDREA, *op. cit.* 450.

[291] https://wikileaks.org/.

[292] Vd. https://wikileaks.org/gifiles/docs/13/1352579_fw-ct-assange-manning-link-not-key-to-wikileaks-case-.html.

[293] In particolare, al centro della vicenda vi è un video che riprende alcuni soldati a bordo di un elicottero fare fuoco su dei civili in Iraq; T BAKKEN, *op. cit.* 8; J L HESTER, *op. cit.* 188.

[294] *Ibidem*, 9; *cfr.* 18 U.S.C. §§ 793(a), §798(a).

[295] *Cfr. New York Times Co. v United States* [1971] 403 U.S. 713, 714; T BAKKEN, *op. cit.* 10; *Unites States v Sterling* [2013] 724 F 3d 482, 492, 499; M PAPANDREA, *op. cit.* 452.

[296] Nel caso *Bartnicki v Vopper* [2001] 532 U.S. 514, la Corte Suprema degli Stati Uniti stabilì che il primo emendamento protegge i *media* che abbiano legalmente ottenuto e pubblicato informazioni, anche laddove la fonte se le fosse procurate illegalmente; T BAKKEN, *op. cit.* 13; la dottrina contraria all'applicazione del primo emendamento nel caso di Assange ritiene invece che questi possa essere penalmente responsabile (ex *Espionage Act §793(a)*) se consapevole che le informazioni erano state ottenute illegalmente dalla fonte e che le stesse potevano essere impiegate a danno degli Stati Uniti: H EDGAR & B C SCHMIDT JR, "The Espionage Statutes and Publication

La proposizione dello SHIELD Act,[297] non fa che confermare questa nuova tendenza: è realmente sentita anche dal potere legislativo l'esigenza di estendere ulteriormente la portata dello *Espionage Act*, così da fornire all' Amministrazione Obama "*increased flexibility to go after WikiLeaks and its founder Julian Assange*." [298] Il progetto di legge, sottoposto ad entrambe le camere del parlamento,[299] per ora rimane dormiente.[300]

7.2. Spie, *leakers, whistleblowers*: le tutele applicabili

Come anticipato, a rivolgersi alla stampa è spesso un impiegato del governo, ma può trattarsi altresì di impiegati presso agenzie per la sicurezza nazionale o di *contractors* (i.e. collaboratori esterni, proprio come Edward Snowden).

Almeno sul piano formale anche al *whistleblower*[301] sono concesse tutele giuridiche, seppur diverse dal quelle del primo emendamento. Quest'ultimo è percepito dalla dottrina maggioritaria come appannaggio della stampa.[302]

Il *Federal Whistleblower Protection Act* 1989 (WPA) effettivamente protegge l'impiegato del governo che abbia rivelato informazioni classificate.[303] Tuttavia, l'ambito di applicazione soggettiva della norma è estremamente ristretto, non ricomprendendo gli impiegati di agenzie di *intelligence*, né i rispettivi *contractors*.[304] Inoltre (salvo casi particolari), gli unici soggetti destinatari della "rivelazione" possono essere l'*Inspector General* (IG) o lo *Special Counsel*.[305] L'indipendenza di entrambe queste figure è piuttosto controversa, dal momento che sono appuntati e rimossi da quello stesso governo che il *whistleblower* ha intenzione di denunciare.[306]

---

of Defense Information" [1973] 73 Colum L Rev 967, 1036; J L HESTER, *op. cit.* 191; M PAPANDREA, *op. cit.* 461.

[297] I.e. *Securing Human Intelligence and Enforcing Lawful Discrimination Act*.

[298] Dichiarazione resa dal Senatore Lieberman, vd. J L HESTER, *op. cit.* 193.

[299] S 315, 112th Cong (2011); HR 703, 112th Cong (2011); J L HESTER, *op. cit.* 193.

[300] M PAPANDREA, *op. cit.* 461-462.

[301] Cd. "vedetta civica".

[302] M PAPANDREA, *op. cit.* 450-451.

[303] La norma pone due limiti essenziali: il tipo di informazioni che possono essere rivelati ed i soggetti destinatari delle rivelazioni. Per una trattazione più approfondita vd. M PAPANDREA, *op. cit.* 491; *cfr.* 5 U.S.C. §2302(b)(8)(A)-(B).

[304] M PAPANDREA, *op. cit.* 492.

[305] *Ibidem*; 5 U.S.C. §20302(b)(8)(B).

[306] M PAPANDREA, *op. cit.* 492.

Lo *Intelligence Community Whistleblower Protection Act* del 1998 risolve solo parzialmente le problematiche esposte. Da un canto, come suggerito dal titolo, viene fornito uno strumento a tutela di quelle categorie escluse dalla legge del 1989. A fare da contraltare, le uniche rivelazioni ammesse da parte di tali soggetti (pena, si ricorda, l'applicazione dello *Espionage Act* §798) sono quelle caratterizzate dal requisito dell'urgenza ("*urgent concern*").[307] Per il resto si ripresenta, acuito, il problema dei soggetti destinatari, dal momento che nessuna informazione può raggiungere il Congresso senza il previo vaglio discrezionale dell'IG.[308]

7.3. Considerazioni

Come si è visto, il diritto statunitense attribuisce la qualifica di *whistleblower* con molta più parsimonia rispetto alla stampa internazionale. Edward Snowden, stando alla lettera della legge, sarebbe piuttosto una spia.

Una simile conclusione però stride con la definizione di spia adottata nella presente trattazione.[309] Sposando le osservazioni di PAPANDREA, si nota che lo spionaggio è connotato da caratteristiche peculiari difficilmente riscontrabili nel caso in esame (e così in altri analoghi). *In primis*, la clandestinità. La raccolta di informazioni da parte della spia non solo avviene in segreto, ma segreta è anche la successiva fase della trasmissione alla potenza straniera.[310] Essendosi rivolto alla stampa nazionale, Edward Snowden è difficilmente paragonabile ad una spia sovietica che trasmette comunicazioni criptate all'URSS.

In termini assoluti, privare i *whistleblowers* della protezione garantita dal primo emendamento, quando si sono serviti del mezzo della stampa, rischia di depauperare l'efficacia sostanziale della norma costituzionale.

Vi è poi una seconda differenza non ininfluente. Si ritiene, infatti, debba esistere un qualche tipo di relazione o accordo tra la spia e la potenza straniera,

---

[307] *I.e.* "a «*serious or flagrant*» *violation of law or executive order, a false statement to the Congress (or willful withholding of information from Congress) or a reprisal against a person who reported the matter of urgent concern"*: M PAPANDREA, *op. cit.* 493; *cfr.* 50 U.S.C. 403q(d)(5)(G)(i).
[308] M PAPANDREA, *op. cit.* 493.
[309] *Cfr.* §1.3.
[310] M PAPANDREA, *op. cit.* 488.

destinataria delle informazioni.[311] Quale che fosse il reale movente di Snowden, l'effetto pratico è stato quello di rendere note sistematiche violazioni del diritto alla *privacy* ai danni di cittadini americani e stranieri.

L'esperienza americana, in questa sede, è stata presa ad esempio per la ricca casistica difficilmente riscontrabile in altri ordinamenti. Sono stati mostrati però anche i limiti intrinseci nel modello statunitense, che soprattutto dopo l'11 Settembre 2001 tende ad anteporre la sicurezza nazionale alle libertà civili.[312]

7.4. Esperienze a confronto: il Consiglio d'Europa

Non si deve pensare che il vecchio continente abbia mancato di disciplinare la pubblicazione di informazioni classificate.[313] Il Consiglio d'Europa, proprio sulla scia del *datagate*,[314] ha adottato da ultimo la Risoluzione 1954 del 2013, intitolata "*National Security and Access to Information*".[315] Questa affronta molte delle problematiche richiamate nei paragrafi precedenti con un approccio profondamente diverso da quello americano.

1) Trasparenza:

Il paragrafo 1 consacra la Risoluzione alla massima accessibilità delle informazioni al fine di garantire la democraticità, il buon governo e per contrastare la corruzione. Si richiama anche la precedente Convenzione CETS 205 del 2009,[316] contenente linee guida in materia di accesso ai documenti ufficiali.[317] Quest'ultima ha il pregio di aver riconosciuto il principio per cui l'accesso ai documenti ufficiali è la regola, mentre il rifiuto costituisce l'eccezione.[318] Inoltre, il diritto di accesso è riconosciuto a "chiunque", senza aver riguardo alle

[311] *Ibidem*.
[312] J C EVANS, "Hijacking Civil Liberties: The USA PATRIOT Act of 2001" (2001-2002) 33 Loy U Chi L J 933-990.
[313] Anche a livello UE sono presenti disposizioni in merito. Tuttavia, essendo queste incentrate sulla trasparenza delle istituzioni europee piuttosto che sugli Stati membri, non saranno trattate in questa sede. Per completezza, si rimanda comunque agli Art. 42 della Carta di Nizza e 15 del TFUE, nonché al Regolamento 1049/2001.
[314] Per provvedimenti più risalenti che hanno ad oggetto la libertà d'espressione, vd. *Committee of Minister Recommendation on "Access to Information Held by Public Authority"* del 1981; *Committee of Ministers Declaration on Freedom of Expression and Information* del 1982.
[315] http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=20190&lang=en.
[316] "*Council of Europe Convention on the Access to Official Documents*": https://wcd.coe.int/ViewDoc.jsp?id=1377737&Site=CM.
[317] Vale a dire, stando all'Articolo 1(2)(a) della Risoluzione: "*all information recorded in any form, drawn up or received and held by public authorities*".
[318] Preambolo, paragrafo 7; Artt. 2 e 3.

motivazioni o alle intenzioni del soggetto interessato.[319] Tuttavia, la Convenzione non è ancora in vigore tra gli Stati Membri del Consiglio d'Europa per la mancanza di quattro ratificazioni.[320]

2) Portata soggettiva:

Dal lato attivo, viene ribadito che il diritto di accesso riguarda "chiunque". Dal lato passivo (*ergo*, chi è tenuto a fornire le informazioni in questione), la Risoluzione adotta una definizione ad ampio spettro. Se da un lato l'autorità pubblica ha sempre il dovere di garantire l'accesso, dall'altro anche "*business enterprises, including private military and security companies, have the responsibility to disclose information in respect of situations, activities or conduct that may reasonably be expected to have an impact on the enjoyment of human rights*".[321]

3) Portata oggettiva:

Posto che anche la Risoluzione ammette deroghe al diritto d'accesso per motivi di sicurezza nazionale,[322] la preoccupazione primaria è stata quella di limitare la portata delle stesse.[323] Su tutti, spicca il paragrafo 9.5.3 che prescrive la prevalenza dell'interesse alla pubblicazione di informazioni che possano rivelare "*serious wrongdoings, including human rights violations, other criminal offences, abuse of public office and deliberate concealment of serious wrongdoing*". E ancora: "*[i]nformation about serious violations of human rights or humanitarian law should not be withheld on national security grounds in any circumstances*".[324] Questa ultima disposizione in particolare, sembra attagliarsi perfettamente alle vicende attuali. Nel caso di Edward Snowden, infatti, la *disclosure* riguardava una probabile violazione strutturale dei diritti umani (*privacy* e dati personali). Nel caso di *Wikileaks*, parimenti, le informazioni diffuse dal soldato Bradley Manning avevano ad oggetto i.a. una probabile violazione del diritto umanitario (uccisione di civili da parte di soldati americani).

4) Tutela dei *whistleblowers*:

[319] Art.1(2)(b).
[320] A fronte delle dieci ratificazioni richieste, solo sei Stati membri hanno provveduto: Bosnia-Erzegovina, Ungheria, Montenegro, Lituania, Finlandia e Svezia.
[321] Risoluzione 1954 (2013), paragrafo 9.1.
[322] Risoluzione 1954 (2013), paragrafo 3.
[323] Risoluzione 1954 (2013), paragrafo 9.
[324] Risoluzione 1954 (2013), paragrafo 9.6.

Già oggetto di una Risoluzione dedicata (la 1729 del 2010), il Consiglio d'Europa torna ad affrontare la questione con rinnovato interesse: "*[a] person who discloses wrongdoings in the public interest (whistle-blower) should be protected from any type of retaliation, provided he or she acted in good faith and followed applicable procedures.*"[325] Anche in questo caso, prevale il principio della sostanza sulla forma. La locuzione "*any type*", infatti, lascia intendere che la tutela garantita debba essere effettiva. Per interpretare correttamente il concetto di *retaliation* (ritorsione) i lavori preparatori [326] rimandano ai cd. *Tshwane Principles,*[327] redatti da *Open Society Foundations* e già richiamati al paragrafo 8 della Risoluzione in esame.[328] "*[Whistleblowers] should be protected from civil or criminal liability, the loss of their job and/or physical and emotional harm*".[329] Inoltre, "*they should not be required to produce documentary evidence for their claims to be investigated or to avoid retaliation, nor should they bear the burden of proof in relation to the veracity of the disclosure, provided they acted in good faith*".[330]

In generale, l'apertura ai *Tshwane Principles* ha un impatto considerevole sulla materia. Pur essendo uno strumento di *soft law*, infatti, i *Principles* contengono una disciplina molto dettagliata alla quale i parlamenti nazionali sono chiamati ad ispirarsi. Sono indicati, i.a. le categorie di informazioni che il *whistleblower* può rivelare,[331] e i casi in cui l'interesse pubblico prevale su quello alla segretezza[332] (vale a dire i punti critici nella legislazione USA). Soprattutto, vengono indicati i principi indefettibili anche qualora debbano essere applicate sanzioni al *whistleblower*: stretta legalità, proporzionalità al danno causato ed esenzione dalla responsabilità penale.[333]

---

[325] Risoluzione 1954 (2013), paragrafo 9.7.
[326] Consiglio d'Europa, Assemblea Parlamentare, Comitato per gli Affari Giuridici e i Diritti dell'Uomo, "National security and Access to Information" [24 Giugno 2013] 20 §89.
[327] *The Global Principles on National Security and the Right to Information* del 12 Giugno 2013. Per maggiori dettagli vd. *infra*.
[328] "*The Assembly supports the Tshwane Principles and calls on the competent authorities of all member States of the Council of Europe to take them into account in modernising their legislation and practice concerning access to information.*"
[329] *The Global Principles on National Security and the Right to Information*, Principio 41.
[330] *Ibidem*, Principio 38.
[331] *Ibidem*, Principio 37.
[332] *Ibidem*, Principio 43.
[333] *Ibidem*, Principio 45.

Infine, si segnala come le presenti norme abbiano influenzato la giurisprudenza della Corte Europea dei Diritti dell'Uomo. Sebbene la CtEDU abbia per diversi anni adottato un'interpretazione restrittiva [334] dell'Art.10 CEDU,[335] di recente si assiste ad un'estensione della materia anche al diritto di accesso e alla tutela del *whistleblower*.

In *Bucur and Toma v. Romania*[336] il ricorrente vide la Corte pronunciarsi (proprio sulla base dell'Art. 10) contro la condanna penale ricevuta in patria per aver divulgato informazioni classificate "*top secret*". Le audiocassette contenenti tali informazioni rivelavano elementi incriminanti a carico di giornalisti e politici.

In *Guja v. Moldova*,[337] la CtEDU dichiarò illegittimo il licenziamento di un procuratore che aveva fornito alla stampa informazioni classificate, le quali rivelavano illecite pressioni politiche sul potere giudiziario. Anche in questo caso la Corte riconobbe una violazione dell'Art. 10 CEDU.

8. Il dualismo nella pratica degli Stati

> *Espionage during a war is justified since it is practised against an enemy; but nations are loathe to admit such a practice in peace-time since "spying" implies enmity when enmity is not officially admitted; it is aimed at breaching the target nation's security which is itself a hostile act.*[338]

Come dimostrano le parole del DO NASCIMENTO, c'è attrito tra pratiche di *intelligence* e principi della Risoluzione 2625 dell'Assemblea Generale.[339] Il

---

[334] *Cfr.* Consiglio d'Europa, Assemblea Parlamentare, Comitato per gli Affari Giuridici e i Diritti dell'Uomo, "National security and Access to Information" [24 Giugno 2013] 9, 10.

[335] "1. Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. Il presente articolo non impedisce agli Stati di sottoporre a un regime d autorizzazione le imprese di radiodiffusione, cinematografiche o televisive.
2. L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario."

[336] *Bucur and Toma v. Romania* (Application no 40238/02) [2013] CEDU.

[337] *Guja v. Moldova* (Application no 142774/04) [2008] CEDU.

[338] G E DO NASCIMENTO, *Diplomacy in International Law* (Kluwer Academic Publiscer, 1973) 61.

[339] A/RES/2625(XXV).

rischio di screditare qualunque tesi a favore della liceità dello spionaggio, nonché dell'*intelligence* in senso lato, è notevole. D'altro canto, bisogna ricordare che la Risoluzione è uno strumento di *soft law* e che trattandosi appunto di una dichiarazione di principi, non può certo avere lo stesso valore di una norma pattizia. Tantomeno può essere invocata come fondamento giuridico per l'attivazione di una procedura di risoluzione delle controversie (es. di fronte alla Corte Internazionale di Giustizia).

È altrettanto vero che la Risoluzione ha in potenza un peso significativo nella determinazione della *opinio juris* esistente, perché espressiva della volontà degli Stati che l'hanno accettata.

Se quindi, giunti a questo punto della trattazione, volessimo ipotizzare l'esistenza di una *opinio juris* contraria quantomeno allo spionaggio (nulla di certo può essere riferito invece all'*intelligence gathering* in generale), non sarebbe comunque possibile risalire ad una regola di diritto consuetudinario. Questo perché la prassi incoerente degli Stati fa venir meno l'elemento della *diuturnitas*, comunque necessario per la formazione di norme consuetudinarie.

Alla luce delle considerazioni svolte in precedenza,[340] *nulla* quaestio sul fatto che gli Stati della comunità internazionale riprovino la conduzione di operazioni di *intelligence* ai propri danni. L'altra faccia della medaglia vede però quegli stessi Stati (palese l'esempio degli Stati Uniti, soprattutto a seguito dello scandalo *datagate*) svolgere attività di *intelligence* anche in tempo di pace, perfino nei confronti di paesi alleati. Senza entrare nel merito di una simile condotta, si prende atto dell'esistenza di una pratica molto più antica della Risoluzione 2625 (XXV).[341] Pertanto, si riconosce l'impossibilità di delineare una prassi coerente. Il giurista non può far altro che seguire i recenti sviluppi tanto in seno all'ONU che all'Unione Europea.[342] In risposta alla vicenda *datagate* infatti, nuovi testi giuridici stanno prendendo forma e nuove dichiarazioni di principi sembrano muoversi nel senso di condannare l'operato delle agenzie di *intelligence* che, dimentiche dei principi di leale collaborazione e buona fede, sorvegliano anche le potenze alleate.

[340] *Cfr.* §2.
[341] Come si è detto *supra*, già nella Bibbia si trovano testimonianze di spionaggio.
[342] Vd. *infra*.

8.1. Giurisdizione extraterritoriale e *protective principle*

A quanto appena asserito in merito al "dualismo" nella pratica generalmente diffusa, si collega una nuova problematica. Gli Stati, si è detto, tradizionalmente condannano le operazioni di *intelligence* (spionaggio, in particolar modo) rivolte ai propri danni. Ciò comporta di regola che le spie straniere siano sottoposte alla giurisdizione nazionale dello Stato *target*. In questo, il destino della spia catturata in tempo di pace, non è dissimile a quello della spia catturata dalla parte belligerante nemica.[343]

1) Nel caso in cui la spia sia catturata mentre si trova ancora nel territorio del *target*, la situazione è pressoché lineare: normalmente lo Stato mandante negherà qualsiasi coinvolgimento con la spia,[344] che verrà dunque giudicata secondo le norme di diritto interno dello Stato spiato.
2) A questo primo scenario più elementare se ne affiancano altri più complessi: ad esempio la spia può essere stata accreditata come agente diplomatico. In questo caso, l'unico rimedio di cui lo Stato offeso dispone consiste nel dichiarare l'agente in questione *persona non grata*.[345] Auspicabilmente, a seguito di ciò lo Stato accreditante richiamerà il "diplomatico-spia", ma nessun rimedio effettivo si rende disponibile allo Stato offeso, vista la natura inviolabile delle immunità diplomatiche.[346]
3) Ancora, è possibile che l'atto di spionaggio sia commesso nello Stato *target*, ma che al momento di perseguire penalmente la spia, questa si trovi nel proprio Stato d'origine. Lo strumento dell'estradizione, che sarebbe la regola in casi analoghi, non può essere impiegato per la mancanza del requisito della doppia incriminazione. Infatti, l'unica sanzione alla quale può essere sottoposto l'agente operativo rientrato in patria, è un provvedimento disciplinare per non aver portato a termine la missione.
4) *Quid*, invece, se l'attività di spionaggio è commessa al di fuori dello Stato *target*? Oltre ad essere commesso da un cittadino straniero, il crimine esula anche dalla giurisdizione territoriale dello Stato spiato. Pure in questo caso le

[343] *Cfr.* capitolo III *infra*.
[344] Salvo casi particolari, tra cui lo *U-2 Incident* per la cui trattazione si rinvia al §2.8.2.
[345] La questione verrà approfondita *infra*, cfr. § 2.5.
[346] CONFORTI B., *Diritto Internazionale* (Editoriale Scientifica, 10° edn, 2014) 258.

autorità pubbliche ben potrebbero avere interesse ad attivarsi al fine di perseguire l'agente. Un rimedio in questi casi esiste, e sarà esaminato di seguito.

8.2. Genesi del protective principle

Nella seconda metà del diciassettesimo secolo, l'Università di Harvard pubblicò una ricerca riguardante la giurisdizione penale in relazione al diritto internazionale.[347] La sua importanza deriva dal fatto che la nomenclatura ivi utilizzata è stata frequentemente adottata sia dai manuali di diritto internazionale, che da varie corti giudicanti. Tra i diversi principi riconosciuti alla base della giurisdizione penale, quello che interessa evidenziare è il *protective principle*, che impiega come criterio attributivo della giurisdizione l'interesse nazionale leso dal reato.[348] Questo ha affiancato, nei paesi dell'Europa Continentale e dell'America Latina, i più comuni criteri territoriali e nazionali. La *ratio* perseguita è la protezione della nazione contro gli atti che ne minacciano la sicurezza.[349]

Inizialmente il *protective principle* era invocabile, in via eccezionale, solo laddove fosse riconosciuto tra l'imputato ed il sovrano un vincolo di lealtà, che si considerava violato con l'atto criminoso.[350] Una simile interpretazione risultava però inconciliabile con l'assetto costituzionale degli Stati Uniti, dove il vincolo era inteso come il rapporto che collega il cittadino americano alla sua nazione.[351] Per questo motivo, la giurisprudenza era sempre stata restia ad esercitare la giurisdizione penale per attività compiute all'estero da imputati stranieri.[352] Solo a seguito di una lenta evoluzione giurisprudenziale, è stato invocato il *protective*

---

[347] M B KRIZEK, "The Protective Principle of Extraterritorial Jurisdiction: a Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice" (1988) 6 B U Int'l L J 337.
[348] M B KRIZEK, *op. cit.* 340.
[349] Gli Stati che basano la loro giurisdizione esclusivamente (o quasi) sui criteri del territorio e della nazione sono una minoranza. *Cfr.* M B KRIZEK, *op. cit.* 340.
[350] Si fa riferimento alla Common Law britannica, che è pur sempre all'origine della tradizione giuridica americana. *Cfr.* M B KRIZEK, *op. cit.* 342.
[351] M B KRIZEK, *op. cit.* 343.
[352] *Cfr. American Banana Co. v. United Fruit Co.* [1909] 213 U.S. 347; *Strassheim v. Daily* [1911] 221 U.S. 280; *United States ex rel. Majka v. Palmer* [1933] 67 F 2d 147; *United States v. Archer* [1943] 51 F Supp 708; *United States v. Bowman* [1922] 260 U.S. 94; *United States v. Baker* [1955] 136 F Supp 546; M B KRIZEK, *op. cit.* 344-345.

principle per poter giudicare un cittadino straniero residente all'estero per atti di spionaggio.

8.3. Continua: United States v. Zehe

Il caso riguarda un cittadino tedesco residente in Messico, Alfred Zehe, accusato dal governo degli Stati Uniti di aver compiuto atti di spionaggio tra il 1982 ed il 1983. La fattispecie integrante reato consisteva nella reiterata trasmissione illegale di documenti secretati dagli USA alla Germania dell'Est.[353] È fondamentale sottolineare che i fatti di cui sopra avevano avuto luogo tra Città del Messico e Berlino Est, ma mai negli Stati Uniti. In forza delle Sezioni 793 e 794 dello *Espionage Act*,[354] le autorità statunitensi arrestarono ed incriminarono Zehe, approfittando della sua momentanea presenza a Boston.

Una simile applicazione extraterritoriale dello *Espionage Act* non sarebbe stata possibile prima del 1961. In quell'anno il Congresso aveva eliminato ogni riferimento all'applicazione territoriale dal testo dello statuto. Dopo il caso Zehe, questo strumento di diritto prettamente interno è stato sfruttato altre volte al fine di contrastare lo spionaggio internazionale.

In prospettiva, si può osservare che le conseguenze pratiche però sono scarse. Limitarsi all'incriminazione o finanche all'arresto della spia rischia di avere poco più che un effetto placebo sull'allarme sociale. Qualora la trasmissione di *intelligence* sia già avvenuta, ciò che davvero conta è agire nei confronti dello Stato mandante, al fine di ottenere riparazione e garanzie di non ripetizione. Nel caso Zehe, oltretutto, nemmeno venne data esecuzione alla pena, ma fu adottata una soluzione sul piano delle relazioni diplomatiche. Nonostante l'imputato si fosse dichiarato colpevole rispetto a tutti i capi d'accusa, fu lasciato in custodia all'ambasciata della Repubblica Democratica Tedesca, ottenendo in cambio il rilascio di diversi cittadini americani trattenuti nella Germania dell'Est.[355]

[353] Per una descrizione più approfondita del fatto, *cfr.* M B KRIZEK, *op. cit.*
[354] Per maggiori dettagli in merito allo *Espionage Act* vd. *infra*.
[355] Questa pratica, denominata comunemente "*tit for tat*", era molto frequente negli anni della Guerra Fredda e fece da epilogo alla cattura di diverse spie sovietiche, cfr. J RADSAN, *op. cit.* 621.

CAPITOLO II – L'UNIONE EUROPEA E GLI STATI UNITI: SCONTRO FRA CULTURE IN MATERIA DI *PRIVACY* E DATI PERSONALI

1. Introduzione

Tra Giugno e Luglio 2013, il quotidiano *The Guardian* ha pubblicato una serie di documenti fatti trapelare da un *contractor* della NSA, Edward Snowden.[356] Questi rivelavano l'esistenza di tre programmi di sorveglianza su vasta scala, condotti di concerto da FBI e NSA.

Il primo prevedeva che Verizon Inc. ed altri gestori telefonici operanti in America fornissero su base giornaliera tutti i metadati delle chiamate dei propri utenti.[357] Un secondo programma, denominato PRISM, forniva alle due agenzie federali completo accesso ai *database* delle principali società americane legate al mondo del web, tra cui Google e Facebook.[358] Secondo le fonti, PRISM è stato operativo ininterrottamente dal 2006.[359] Il terzo programma, XKeyscore, consisteva nella collezione indiscriminata di metadati (generati i.a. da e-mail, chat, navigazione *online*) avvalendosi di una rete di oltre cinquecento *server* segreti.[360]

Nel Regno Unito la GCHQ (i.e. *Government Communications Head Quarter*, la principale agenzia di *intelligence* britannica), avrebbe prestato il proprio contributo al programma PRISM collocando dei dispositivi di ricezione direttamente sui cavi in fibra ottica che trasmettono dati attraverso l'Atlantico. L'operazione è nota col nome in codice *Tempora*.[361]

In Francia, anche la DGSE (*Direction Générale de la Sécurité Extérieure*) attraverso la sorveglianza elettronica avrebbe intercettato illegalmente comunicazioni telefoniche e via Internet in modo indiscriminato ed estensivo.[362]

Il susseguirsi di queste ed altre notizie analoghe ha dato forma allo scandalo conosciuto come *datagate*. Tanto le istituzioni internazionali, quanto quelle

---

[356] D GRAY & D CITRON: "The Right to Quantitative Privacy" (2013) 98 Minn L Rev 63.
[357] *Ibidem*.
[358] Tra le altre figurano Microsoft, Apple, Skype, Yahoo! e AOL. Le società coinvolte hanno negato pubblicamente la propria collaborazione; *cfr. Ibidem*.
[359] NINO M., *op. cit.* 736.
[360] D GRAY & D CITRON, *op. cit.* 64.
[361] NINO M., *op. cit.*
[362] *Ibidem*.

europee e statali hanno improvvisamente realizzato quale sia il potenziale di un simile "leviatano digitale". Di conseguenza, hanno prontamente coordinato i propri sforzi al fine di contrastare il fenomeno della *mass surveillance*.

Il presente capitolo si concentrerà sull'impatto che l'attività di *intelligence* ha sul dritto alla *privacy* dei cittadini. Per farlo, verranno messi a confronto i due principali attori dell'odierno dibattito globale: Stati Uniti e UE. Come si avrà modo di appurare, negli USA le agenzie federali trovano terreno fertile per attuare programmi come PRISM. Questo perché il sistema normativo è disarticolato e disomogeneo, nonché facilmente derogabile in nome della lotta al terrorismo internazionale.[363] Ciononostante, non si deve credere che la legittimità di simili programmi sia salva da qualunque criticismo: anche in patria, diverse associazioni per i diritti civili e parte della giurisprudenza si battono per affermarne l'incompatibilità con la Costituzione.[364]

In primo luogo saranno passate in rassegna le principali convenzioni internazionali in materia di diritti umani. Così facendo saranno enucleati i principi cardine che entrambi i continenti occidentali sono tenuti a rispettare per ciò che concerne *privacy* e tutela dei dati personali. L'analisi si sposterà dunque sull'Europa, dove Consiglio d'Europa e UE hanno operato armoniosamente per affermare i diritti fondamentali della persona. Le tutele previste tanto dalle convenzioni internazionali che dall'*acquis* delle due organizzazioni regionali sono sovrapponibili e formano un solido impianto normativo.[365]

Il risultato è quello di avere in Europa e negli USA due concezioni (*rectius* interpretazioni di un medesimo concetto) molto differenti in materia di *privacy* e tutela dei dati personali. Tuttavia nella odierna società digitale, in cui l'America detiene di fatto la *governance* esclusiva del Web, i superiori standard di protezione garantiti dall'UE sono fortemente sviliti. Infatti, tutti i dati che transitano per i *server* statunitensi (quindi la maggior parte di essi) ad oggi possono essere soggetti a controlli arbitrari.

[363] *Ibidem*, 727.
[364] Vd. *infra*.
[365] *Cfr*. NINO M., *op. cit.*

Nella parte finale del capitolo verranno riportate alcune proposte finalizzate proprio a colmare tale *gap* normativo e a ravvicinare, per quanto possibile, gli standard di tutela offerti nei due continenti occidentali.

2. Il quadro normativo

2.1. Convenzioni internazionali e *soft law*

2.1.1. La Dichiarazione Universale dei Diritti dell'Uomo

La Dichiarazione Universale dei Diritti dell'Uomo è stata adottata dall'Assemblea Generale delle Nazioni Unite il 10 Dicembre 1948.[366] Si tratta di una statuizione solenne, che trova applicazione in tutti gli Stati membri dell'ONU. Parimenti, è la fonte più risalente in materia di *privacy* e tutela dei dati personali intesi come diritti umani. L'Art. 12 della Dichiarazione dispone che:

> [n]essun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni.[367]

Pur essendo priva di vincolatività, la norma costituisce un punto di partenza essenziale per tutti gli strumenti legislativi che l'anno seguito ed ha un notevole impatto sulla *opinio juris* globalmente diffusa.

Un secondo pregio è quello di enucleare già due elementi portanti della disciplina: il requisito della non arbitrarietà di eventuali interferenze ed il diritto ad una tutela legale contro le stesse.

Nei paragrafi successivi saranno descritte le diverse modalità di recepimento di questi principi e la loro evoluzione.

2.1.2. Il Patto internazionale sui Diritti Civili e Politici

L'Art. 17 del Patto internazionale relativo ai Diritti Civili e Politici (ICCPR) stabilisce che:

[366] http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=itn.
[367] *Ibidem*, Art. 12.

1. Nessuno può essere sottoposto ad interferenze arbitrarie o illegittime nella sua vita privata, nella sua famiglia, nella sua casa o nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione.

2. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze od offese.[368]

Insieme alla Dichiarazione Universale, si tratta della norma internazionale in materia di *privacy* di più ampia adesione.[369]

Pur essendo ricognitivo di diversi principi fondamentali dalla portata generalissima, è errato ritenere che il Patto contenga mere norme programmatiche. Innanzitutto, il commento generale[370] dello *Human Rights Committee* (HRC)[371] è utile per comprendere l'esatto significato della disposizione.

Per interferenze "illegittime", si intende che:

no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.[372]

Posto che una simile ingerenza sia autorizzata dalla legge, questa può ancora essere in contrasto con le prescrizioni del Patto laddove sia "arbitraria", dal momento che:

even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.[373]

I principi di legalità e non arbitrarietà, così descritti, sono i pilastri su cui si regge l'intera disciplina e che ispirano l'approccio delle istituzioni europee alla *privacy*.[374]

---

[368] Patto internazionale relativo ai Diritti Civili e Politici, New York, 1966.

[369] Il Patto conta alla data odierna 168 Stati parti; vd. https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en.

[370] OHCHR, *General Comment* No. 16: "Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation)" [1988] HRI/GEN/1/Rev.9 (Vol. I).

[371] Vd. http://www.ohchr.org/en/hrbodies/ccpr/pages/ccprindex.aspx.

[372] HRI/GEN/1/Rev.9 (Vol. I), §4.

[373] *Ibidem*, §3.

[374] Vd. *infra*.

Proseguendo con la lettura in chiave interpretativa dell'Art. 17, emergono altri elementi di notevole rilevanza per la presente trattazione. Infatti:

> *[c]ompliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto.* […] *Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.*[375]

Un simile riferimento all'attività di sorveglianza elettronica si attaglia perfettamente alle vicende attuali e consente di affermare con un certo grado di sicurezza che l'attività perpetrata dalla NSA è in netto contrasto con le previsioni dello ICCPR. Come si avrà modo di approfondire in seguito, se pure i programmi di *bulk data collection* fossero formalmente legali in forza del diritto statunitense (ma il punto è controverso dalla stessa giurisprudenza americana), difficilmente se ne può sostenere la non arbitrarietà. Infatti, stando alle rivelazioni di Snowden, i metadati di milioni di individui sono stati carpiti in massa, senza una reale necessità a monte e senza garantire minimamente alle persone interessate il diritto di accesso.[376]

Durante la trentacinquesima Conferenza internazionale dei Garanti per la *privacy* (tenutasi a Varsavia tra il 23 ed il 26 Settembre 2013),[377] l'importanza dello ICCPR non è stata ignorata. I partecipanti hanno adottato una Risoluzione[378] che invita i governi nazionali all'elaborazione di un Protocollo Addizionale all'Art. 17 "*which should be based on the standards that have been developed and endorsed by the International Conference and the provisions in General Comment No. 16 to the Covenant in order to create globally applicable standards for data protection and the protection of privacy in accordance with the rule of law*."[379] Anche la relazione del Comitato LIBE del Parlamento europeo, già menzionata in precedenza, esorta gli Stati membri dell'Unione a seguire il dettato della

[375] HRI/GEN/1/Rev.9 (Vol. I), §8.
[376] La portata del diritto di accesso verrà illustrata *infra*; *cfr*. HRI/GEN/1/Rev.9 (Vol. I), §10.
[377] https://privacyconference2013.org/.
[378] Resolution on Anchoring Data Protection and the Protection of *Privacy* in International Law, 35th International Conference on Data Protection and Privacy Commissioners (Warsaw, 23-26 September 2013): https://privacyconference2013.org/web/pageFiles/kcfinder/files/5.%20International%20law%20resolution%20EN%281%29.pdf.
[379] *Ibidem*.

Risoluzione al fine di rispondere all'emergenza che riguarda gli strumenti di sorveglianza.[380]

La grande attenzione rivolta al Patto ha probabilmente una causa duplice. *In primis*, come si è detto, è lo strumento internazionalmente più diffuso a garantire una disciplina coesa in materia di *privacy*. Vi hanno aderito tanto gli USA quanto i paesi UE, fornendo dunque una base giuridica per il dialogo tra le due parti.

In secondo luogo, lo strumento offre maggiori possibilità di garantire l'attuazione effettiva delle proprie norme. L'Art. 41, che predispone una *complaint procedure*, recita:

> [o]gni Stato parte del presente Patto può dichiarare in qualsiasi momento, in base al presente articolo, di riconoscere la competenza del Comitato a ricevere ed esaminare comunicazioni, nelle quali uno Stato parte pretenda che un altro Stato parte non adempie agli obblighi derivanti dal presente Patto.[381]

Il Comitato, accertato il previo esaurimento dei ricorsi interni disponibili, entra nel merito della questione.[382] Se le parti rifiutano una soluzione amichevole,[383] viene redatto entro dodici mesi un rapporto, al quale le parti controvertenti devono attenersi.[384]

2.1.3. Risoluzione dell'Assemblea Generale: *The Right to Privacy in the Digital Age*

Come reso noto nel capitolo precedente, durante la sessantottesima sessione dell'Assemblea Generale delle Nazioni Unite è stata adottata la versione definitiva della Risoluzione "*The Right to Privacy in the Digital Age*".[385] Si tratta di una prima risposta concreta dell'ONU alla vicenda *datagate* e mostra una inequivocabile natura garantista, trainata dai paesi più colpiti dall'attività di SIGINT americana.

---

[380] European Parliament – Committee on Civil Liberties, Justice and Home Affairs, Report (2013/2188(INI)) §128.
[381] Patto internazionale relativo ai Diritti Civili e Politici, Art. 41(1).
[382] *Ibidem*, Art. 41(1)(c).
[383] *Ibidem*, Art. 41(1)(e).
[384] *Ibidem*, Art. 41(1)(h); nel caso in cui non venga trovata una soluzione soddisfacente, può essere istituita una Commissione *ad hoc* ex Art. 42.
[385] A/RES/68/167.

Nelle *preambulatory clauses* vengono invocati i.a. i testi normativi appena esaminati: l'Art. 12 della Dichiarazione Universale dei Diritti dell'Uomo e l'Art. 17 del Patto Internazionale sui Diritti Civili e Politici.[386] Soprattutto, vengono riaffermati i principi-cardine che proibiscono l'ingerenza illegale od arbitraria nella vita privata degli individui.

Inoltre, l'Assemblea Generale dichiara di accogliere i risultati del rapporto sottoposto allo *Human Rights Council* da Frank La Rue, relativo all'impatto delle nuove tecnologie sulla libertà d'espressione.[387] Questo notava come la capacità degli Stati di intercettare le comunicazioni private dei cittadini, in nome della sicurezza nazionale, sia cresciuta esponenzialmente negli anni.[388] In particolar modo, è cambiata la natura dei dati sottoposti al controllo statale: i metadati possono rivelare una moltitudine d'informazioni, dalla posizione geografica dell'individuo all'identità del mittente di una e-mail.[389] I cambiamenti rivoluzionari quanto frequenti che contraddistinguono le tecnologie informatiche hanno inevitabilmente condizionato la percezione dei confini tra sfera pubblica e privata.[390] Il giudizio di La Rue è che, nel complesso, i legislatori nazionali non siano riusciti a tenere il passo con lo sviluppo crescente.[391] Le criticità maggiori riguardano proprio l'attività di sorveglianza *en masse*:

> *communications surveillance can also be authorized on a broad and indiscriminate basis, without the need for law enforcement authorities to establish the factual basis for the surveillance on a case-by-case basis.*[392] *[…] Even when judicial authorization is required by law, often it is de facto an arbitrary approval of law enforcement requests.*[393]

[386] *Cfr. supra*.
[387] F LA RUE, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" [2013] A/HRC/23/40.
[388] *Ibidem*, §12.
[389] *Ibidem*, §15.
[390] *Ibidem*, §21, 33.
[391] *Ibidem*, §50.
[392] *Ibidem*, §54.
[393] *Ibidem*, §56.

In particolar modo, le agenzie di *intelligence* godono spesso di autorizzazioni "in bianco". Si tratta di un problema comune, non circoscritto alla situazione negli USA.[394]

La Risoluzione 68/167 si riallaccia a queste premesse, incentivando gli Stati membri al rispetto della *privacy* come diritto di ogni individuo. Ciò deve essere valido sia *online* che *offline*, in modo coerente con gli obblighi assunti per la tutela dei diritti umani.[395] È altresì demandata l'istituzione (per quei paesi che già non ne dispongano) di meccanismi di controllo indipendenti che garantiscano la trasparenza delle attività di sorveglianza statali.[396]

Come anticipato nel capitolo precedente,[397] è stato anche richiesto all'Alto Commissario per i diritti umani di presentare un rapporto. L'oggetto della ricerca è l'attività di sorveglianza (anche su larga scala) compiuta all'interno della giurisdizione nazionale od in modo transfrontaliero.[398] Il progetto è stato sviluppato tra Novembre 2013 e Marzo 2014 ed ha coinvolto attivamente anche gli Stati membri tramite le rappresentanze permanenti a New York e Ginevra.[399]

Esattamente come per la Risoluzione 68/167, il rapporto prende le mosse dal dettato dell'Art. 17 ICCPR, letto attraverso l'interpretazione fornita dal commento generale No. 16.[400] La trattazione, dunque, è nuovamente incentrata sulle nozioni di non arbitrarietà e legalità delle intercettazioni.[401] Queste vengono poste in stretta relazione con i principi di necessità e proporzionalità:

---

[394] F LA RUE, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" [2013] A/HRC/23/40/Corr.1: "*in the United States, the Foreign Intelligence Surveillance Act empowers the National Security Agency to intercept communications without judicial authorization where one party to the communication is located outside the United States, and one participant is reasonably believed to a member of a State-designated terrorist organization. German law allows warrantless automated wiretaps of domestic and international communications by the State's intelligence services for the purposes of protecting the free democratic order, existence or security of the State. In Sweden, the Law on Signals and Intelligence allows for the interception of communications after authorization by the Foreign Intelligence Court. In the United Republic of Tanzania, the Intelligence and Security Service Act 1996 enables the country's intelligence services to conduct any investigations and investigate any person or body which it has reasonable cause to consider a risk or a source of risk or a threat to the State security.*"
[395] A/RES/68/167, §4(c).
[396] *Ibidem*, §4(d).
[397] *Cfr.* capitolo precedente.
[398] A/RES/68/167, §5.
[399] A/HRC/27/37, §8-9.
[400] *Ibidem*, §17.
[401] *Ibidem*, §21-27.

any limitation to privacy rights reflected in article 17 must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances. The limitation must be necessary *for reaching a legitimate aim, as well as* in proportion *to the aim and the least intrusive option available.*[402] (Enfasi aggiunta).

Per queste ragioni, programmi di sorveglianza in massa (*bulk data collection*) devono essere considerati arbitrari in ogni caso, anche qualora servano uno scopo legittimo e siano stati adottati sulla base di una norma accessibile e trasparente.[403] Allo stesso tempo leggi segrete o strumenti analoghi, anche se soggetti al vaglio giurisdizionale, non vanno considerati "leggi" in senso proprio[404] e non possono essere invocati per giustificare simili attività.

Un altro spunto interessante riguarda l'estensione della protezione garantita dallo ICCPR. Come è noto, l'Art. 2(1) del Patto impone allo Stato membro di garantire i diritti in esso riconosciuti solamente alle persone "che si trovino sul suo territorio". Ciononostante, la giurisprudenza dello *Human Rights Committee* sostiene da diverso tempo che "*a State may not avoid its international human rights obligations by taking action outside its territory that it would be prohibited from taking «at home»*."[405] L'Art. 2(1) ICCPR, in sostanza, non ostacola l'applicazione del Patto a chiunque si trovi sotto il controllo effettivo dello Stato contraente.[406] Solo così è rispettato il principio di non discriminazione.[407]

Per quanto riguarda il controllo giurisdizionale sull'attività di sorveglianza, viene ribadito quanto già sostenevano Frank La Rue ed il precedente *Special Rapporteur* Martin Scheinin:[408] l'autorità giudiziaria che vigila sull'operato delle

[402] *Ibidem*, §23; *cfr*. CCPR/C/21/Rev.1/Add.9, §§11 – 16; A/HRC/14/46, annex, practice 20.
[403] A/HRC/27/37, §25.
[404] *Ibidem*, §29.
[405] *Ibidem*, §33; *Official Records of the General Assembly, Thirty-sixth Session, Supplement No. 40* (A/36/40) annex XIX, §§ 12.2-12.3, annex XX, §10.3.
[406] A/HRC/27/37, §31; CCPR/C/21/Rev.1/Add.13, §10; A/36/40, annex XIX §12.2, annex XX; CCPR/CO/78/ISR §11; CCPR/CO/72/NET, §8; CCPR/CO/81/BEL, §6; Inter-American Commission of Human Rights, *Coard & al. v. United States*, case No. 10.951, Report No. 109/99 [1999] §§37, 39, 41, 43.
[407] A/HRC/27/37, §36.
[408] M SCHEININ, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism" [2009] A/HRC/13/37, §67.

forze di polizia o delle agenzie di *intelligence* deve poter agire in piena indipendenza.[409]

Infine, l'Alto Commissario evidenzia l'importanza di predisporre ricorsi efficaci per le persone ingiustamente colpite dall'ingerenza dei pubblici poteri.[410] Il primo passo è ovviamente la cessazione delle violazioni ancora in corso.[411] Dopodiché, quale che sia la forma del rimedio disponibile, è fondamentale che questo sia accessibile, i.e. conoscibile e facilmente esperibile.[412] Viene consigliata l'istituzione di organi di vigilanza all'uopo preposti, che nel rispetto dei principi del giusto processo[413] possano accertare i fatti, porre fine alle violazioni accertate ed emettere ordinanze vincolanti.[414] Nel caso di violazioni gravi e sistematiche, si suggerisce la predisposizione di strumenti di diritto penale.[415]

2.2. La normativa UE e CEDU

2.2.1. Il Concetto di *Habeas Data* in Europa

Il concetto di *habeas data* (letteralmente, "che tu abbia i dati") si ricollega ad una garanzia costituzionale introdotta in tempi relativamente recenti negli ordinamenti giuridici latinoamericani.[416]

Per comprenderne il significato è opportuno richiamare un diritto ben più antico, mutuato dalla tradizione anglosassone, ed incorporato nel noto *writ of habeas corpus*.[417] In origine, tale *writ* tutelava la libertà personale del suddito

---

[409] *Ibidem*; A/HRC/27/37, §38.
[410] Patto Internazionale relativo ai Diritti Civili e Politici, Art. 2(3)(b): "[Ciascuno degli Stati parti del presente Patto s'impegna a] garantire che l'autorità competente, giudiziaria, amministrativa o legislativa, od ogni altra autorità competente ai sensi dell'ordinamento giuridico dello Stato, decida in merito ai diritti del ricorrente, e sviluppare le possibilità di ricorso in sede giudiziaria."
[411] A/HRC/27/37, §39.
[412] *Ibidem*, §40.
[413] *Ibidem*, §41; OAS, "Joint declaration on surveillance programs and their impact on freedom of expression", issued by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (June 2013) §9: www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1.
[414] A/HRC/27/37, §41, A/HRC/14/46.
[415] A/HRC/27/37, §41; A/RES/60/147 annex, Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law.
[416] RUSSO S., *Habeas Data e Informatica* (Giuffrè, edn, Milano) 12; BORREA ODRÌA A., *Las garantìas constitucionales: habeas corpus y amparo*, Lima, Libros Peruanos, 1992.
[417] RUSSO S., *op. cit.* 3; ROZO ACUÑA E., *Habeas Data costituzionale: nuova garanzia costituzionale del diritto pubblico latinoamericano*, in *Diritto pubblico comparato ed europeo*,

contro l'arbitrario esercizio del potere sovrano.[418] Oggi consente in concreto l'avvio di un procedimento giudiziario ogniqualvolta un individuo si veda privato della propria libertà personale, a qualsiasi titolo.[419]

Nell'era digitale, la persona non è più soltanto entità fisica. Ancor prima di accedere volontariamente alla rete, tutti posseggono ormai una propria identità digitale, che si può estrinsecare tanto in una scheda anagrafica informatizzata quanto nell'account di un *social network*. Ecco allora nascere l'esigenza di tutelare l'autodeterminazione dell'io digitale, da cui discende il concetto di *habeas data*. In modo del tutto analogo all'*habeas corpus*, esso subordina ogni sorta di atto limitativo della libertà informatica all'emanazione di un provvedimento giudiziario.

Curiosamente, i paesi dell'America Latina sono stati precursori nello studio di questi "nuovi diritti",[420] ed hanno modellato il proprio assetto costituzionale di conseguenza.[421] Tra tutte, merita di essere richiamata la *Constituição Cidadã* del Brasile, visto il ruolo portante che il paese ha avuto nel dibattito internazionale sulla *bulk data collection*. L'Art. 5(LXXII) della Costituzione in esame prevede una specifica azione di *habeas data*,[422] la quale assicura all'interessato l'accesso alle informazioni che lo riguardano. Queste devono essere state archiviate in banche dati governative o appartenenti ad agenzie pubbliche. Non solo: all'interessato è riconosciuto anche il diritto di rettifica, volto a modificare il contenuto di dati non aggiornati od incorretti. In un sistema giuridico come quello brasiliano la raccolta massiva di metadati dei cittadini, operata senza garantire loro l'accesso ai medesimi, non solo è incostituzionale: è inconcepibile.

La dottrina[423] ha ipotizzato che anche in Europa e nei singoli Stati membri sia possibile riscontrare, attraverso l'interpretazione estensiva, norme

---

2002-IV, Giappichelli, Torino, 1923ss; ROZO ACUÑA E., voce *Habeas Corpus (America Latina)*, nel *Digesto IV ed., Disc. pen.*, Aggiornamento I, Utet, 2005, 669.

[418] *Ibidem*; W S HOLDSWOTH, *A History of English Law Vol. IX* (London, 1924) 114.

[419] RUSSO S., *op. cit.* 5; *Administration of Justice Act* 1960.

[420] RUSSO S., *op. cit.* 115; ROZO ACUÑA E., *op cit*.

[421] *Cfr*. i.a. Costituzione del Guatemala, Art. 35; Costituzione del Paraguay, Art. 135; Costituzione argentina, Art. 43; Costituzione del Costa Rica, Art. 30, 48; Costituzione brasiliana, Art. 5.

[422] L COSTA, "A Brief Analysis of Data Protection Law in Brazil" [2012] Presented to the Consultative Committee of the Convention for Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD) 6.

[423] RUSSO S., *op. cit.* 121.

riconducibili all'*habeas data*. Per quanto riguarda il Consiglio d'Europa, esiste un fondamento normativo nell'Art. 8 CEDU, che recita:

> 1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.
>
> 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

La disposizione non fa riferimento esplicito all'istituto in esame, né al diritto alla *privacy* o alla tutela dei dati personali. Tuttavia negli anni il diritto alla vita privata e familiare ha subito un'evoluzione notevole, veicolata dalla giurisprudenza della CtEDU. In questo modo, l'articolo è arrivato ad abbracciare tematiche molto più vaste.[424] A seguire verranno analizzati due casi in cui l'Art. 8 è stato invocato avverso l'ingerenza dei servizi segreti, con esiti diversi.

In *Leander v. Sweden*,[425] il ricorrente vedeva rifiutata la sua domanda di assunzione presso un museo situato in una base navale militare. Infatti, il datore di lavoro aveva appreso tramite un fascicolo, raccolto dai servizi segreti svedesi, che Leander aveva precedentemente militato nel partito comunista locale ed aveva svolto attività sindacale. Ciò lo rendeva inidoneo. La Corte stabilì che effettivamente esisteva un'ingerenza ex Art. 8(1) CEDU, poiché le informazioni erano state raccolte e trasmesse senza darne comunicazione al ricorrente e senza lasciargli la possibilità di confutarne il contenuto. Tuttavia, nel caso di specie non fu riscontrata alcuna violazione della Convenzione. Le misure adottate, infatti, furono considerate proporzionate e necessarie per la tutela dell'interesse alla sicurezza nazionale.

In *Amann v. Switzerland*,[426] al contrario, la Corte condannava il governo svizzero per la mera detenzione di un fascicolo classificato che conteneva

[424] E.g. in materia di integrità fisica vd. *X and Y v. Netherlands* (Application no 8978/90) [1985] CEDU; *Costello-Roberts v. United Kingdom* (Application no 13134/87) [1993] CEDU.
[425] *Leander v. Sweden* (Application no 9248/81) [1987] CEDU.
[426] *Amann v. Switzerland* (Application no 27798/95) [2000] CEDU.

informazioni sul ricorrente. Il dossier era stato raccolto dai servizi segreti nel 1981, nel corso di un'indagine su possibili legami tra Amann e l'Unione Sovietica. Il trattamento dei dati in questione fu giudicato contrario al dettato dell'Art. 8 CEDU, perché non giustificato da specifiche disposizioni di diritto interno. Per di più, il codice di procedura penale svizzero dispone espressamente che le informazioni acquisite nell'ambito di una sorveglianza approvata ma non più necessaria debbano essere distrutte non appena si sia chiuso il procedimento.[427]

Nonostante le due pronunce prendano direzioni diverse, esse esprimono uno stesso principio: anche nell'ordinamento CEDU l'individuo ha diritto al ricorso giurisdizionale contro i provvedimenti afflittivi della libertà informatica, con modalità che ricalcano considerevolmente l'*habeas data*. La libertà della persona può soccombere, ma solo di fronte ad un provvedimento adottato nell'interesse nazionale, che rispetti i principi di proporzionalità e stretta legalità.

La medesima dottrina[428] riconosce anche in Italia la presenza di norme riconducibili all'*habeas data*. La teoria prende le mosse dal combinato disposto degli Artt. 2[429] e 13[430] Cost. e dalla Sentenza 38/1973 della Corte Costituzionale. Il giudice delle leggi, diversi anni prima della redazione di norme sulla *privacy*, già riconosceva che il nostro ordinamento garantisce taluni "diritti inviolabili dell'uomo, fra i quali rientra quello del proprio decoro, del proprio onore, della propria rispettabilità, *riservatezza, intimità* e reputazione, sanciti espressamente dagli articoli 8 e 10 della Convenzione dei diritti dell'uomo" (enfasi aggiunta).[431] Così pure la Sentenza 139/1990 già definiva lo scopo della tutela della *privacy* nel "prevenire qualsiasi rischio che i dati raccolti siano conosciuti all'esterno nel loro

[427] Codice di Diritto Processuale Penale Svizzero, Artt. 269ss.
[428] RUSSO S., *op. cit.* 17.
[429] "La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale."
[430] "La libertà personale è inviolabile. Non è ammessa forma alcuna di detenzione, di ispezione o perquisizione personale, né qualsiasi altra restrizione della libertà personale, se non per atto motivato dell'Autorità giudiziaria e nei soli casi e modi previsti dalla legge. In casi eccezionali di necessità ed urgenza, indicati tassativamente dalla legge, l'autorità di Pubblica sicurezza può adottare provvedimenti provvisori, che devono essere comunicati entro quarantotto ore all'Autorità giudiziaria e, se questa non li convalida nelle successive quarantotto ore, si intendono revocati e restano privi di ogni effetto. È punita ogni violenza fisica e morale sulle persone comunque sottoposte a restrizioni di libertà. La legge stabilisce i limiti massimi della carcerazione preventiva."
[431] Corte Costituzionale, Sentenza n 38/1973 del 5 Aprile 1973; RUSSO S., *op. cit.* 29.

riferimento nominativo o individuale ovvero in modo tale che siffatto riferimento possa essere riconosciuto pur in presenza di dati anonimi o aggregati".[432]

Ciò che manca in Italia è la possibilità di un ricorso diretto come l'azione di *habeas data* o il *recurso de amparo*, al fine di chiedere al giudice costituzionale la tutela dei diritti appena elencati. Nel nostro ordinamento questo vuoto è parzialmente colmato dalla Corte di Cassazione, che in diverse occasioni si è allineata alle posizioni della Corte Costituzionale menzionate in precedenza. Nella Sentenza 3769/1995 Cass. civ. si legge che "la finalità dell'art. 2 Cost. è quella di tutelare la persona umana integralmente e in tutti i suoi modi di essere essenziali. Tale norma costituzionale non ha una funzione meramente riassuntiva dei diritti espressamente garantiti nel testo costituzionale od anche di quelli inerenti alla persona umana previsti nel codice civile; essa si colloca al centro dell'intero ordinamento costituzionale e assume come punto di riferimento la persona umana nella complessità ed unitarietà dei suoi valori e bisogni, materiali e spirituali. Appunto perciò la norma non può avere un contenuto soltanto riepilogativo; essa costituisce una clausola aperta e generale di tutela del libero ed integrale svolgimento della persona umana."[433] Così la Cassazione penale, nella Sentenza 878/1996, riconduceva il diritto all'identità personale "direttamente all'art. 2 Cost. inteso tale precetto nella sua più ampia dimensione di clausola generale aperta all'evoluzione dell'ordinamento e suscettibile, per ciò appunto, di apprestare copertura costituzionale ai nuovi valori emergenti della personalità, in correlazione anche all'obiettivo primario di tutela del pieno sviluppo della persona umana, di cui al successivo art. 3 cpv."[434]

Anche in ambito UE, in tempi recenti, si comincia a teorizzare un *habeas corpus* digitale europeo. Il rapporto del comitato LIBE, già menzionato in precedenza,[435] ne propone l'implementazione attraverso un "*priority plan"* diviso in otto punti programmatici.[436] In breve, questi sono mirati a:

[432] Corte Costituzionale, Sentenza n 139/1990 del 7 Marzo 1990; RUSSO S., *op. cit.* 32.
[433] Corte di Cassazione, Cass. Civ., Sez. I, 22 Giugno 1995 n. 3769; RUSSO S., *op. cit.* 32-33.
[434] Corte di Cassazione, Cass. pen., Sez. I, 9 Febbraio 1996 n. 878; Corte di Cassazione, Cass. Civ., Sez. I, 22 Giugno 1995 n. 3769; RUSSO S., *op. cit.* 33.
[435] European Parliament, Report (2013/2188(INI)).
[436] *Ibidem*, 43.

1) Adottare il pacchetto legislativo sulla protezione dei dati personali[437] entro il 2014.
2) Concludere l'accordo tra USA e UE denominato *Umbrella Agreement.*[438]
3) Sospendere il *Safe Harbor* fino a che non siano stati risolti i difetti noti.
4) Sospendere il TFTP[439] fino a quando non sarà conclusa un'indagine approfondita in merito e comunque fino all'adozione dello *Umbrella Agreement*.
5) Valutare ogni accordo esistente che comporti lo scambio di dati con paesi terzi, al fine di assicurare l'assenza di ingerenze legate ad attività di sorveglianza. Si raccomandano anche successive procedure di *follow-up*.
6) Proteggere lo Stato di diritto ed i diritti fondamentali dei cittadini europei, i.a. la libertà d'espressione, il segreto professionale ed una protezione rafforzata per i *whistleblowers*.
7) Sviluppare una strategia per ottenere maggior indipendenza informatica a livello europeo. Si mira ad un cd. *New Deal* digitale,[440] capace di accrescere l'autonomia dell'Unione Europea attraverso tecnologie proprie,[441] combinate ad alti livelli di protezione dei dati personali.
8) Rendere l'Unione Europea il punto di riferimento per un'amministrazione neutrale e democratica dell'Internet.

L'istituto dell'*habeas data*, come si è visto, è poliedrico e dinamico.[442] Si ricollega a tutta una serie di diritti tra loro interconnessi: i.a. *privacy,* tutela dei dati personal e dignità personale. In più, agli aspetti di diritto sostanziale se ne

[437] Si tratta di un pacchetto contenente sia il Regolamento Generale sulla Protezione dei Dati Personali, che una nuova Direttiva volta a disciplinare i trattamenti per finalità di giustizia e polizia (oggi trattati nella Decisione-Quadro 2008/977/GAI); vd. Proposta di Direttiva del Parlamento Europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati, 25 Gennaio 2012, COM(2012) 10 final.
[438] Per l'analisi dello *Umbrella Agreement*, si rinvia *infra*.
[439] I.e. *Terrorist Finance Tracking Program*: programma in forza del quale al governo statunitense è consentito l'accesso si server SWIFT che elaborano i dati di messaggistica finanziaria dall'UE agli USA; vd. anche Parlamento Europeo, proposta di risoluzione comune sulla sospensione dell'accordo TFTP a seguito della sorveglianza dell'Agenzia per la sicurezza nazionale statunitense, 21 Ottobre 2013, (2013/2831(RSP)).
[440] *Cfr*. European Parliament – Committee on Civil Liberties, Justice and Home Affairs, "NSA snooping: MEPs table proposals to protect EU citizens' privacy" (12/2/2014).
[441] Ad esempio, nuove soluzioni di *cloud computing* sviluppate unicamente all'interno dell'Unione.
[442] RUSSO S., *op. cit.* 128.

affiancano altri processuali: la possibilità di chiedere la tutela giurisdizionale di quegli stessi diritti o perfino di promuovere un ricorso immediato di fronte alla Corte Costituzionale. Un istituto, dunque, che è possibile innestare (con uno sforzo ermeneutico minimo) tanto negli ordinamenti dell'America Latina che in quelli europei.

2.2.2. Il Consiglio d'Europa: Art. 8 CEDU, Convenzione 108 e nuove proposte normative

Come appurato *supra*, il Consiglio d'Europa ha sviluppato negli anni un solido *acquis* in materia di *privacy* e tutela dei dati personali. Il tentativo di operare un bilanciamento tra questi diritti e le esigenze di sicurezza nazionale ne è parte integrante. Già diversi anni prima delle sentenze *Leander* e *Amann* (nonché dell'intera vicenda *datagate*), la Corte di Strasburgo affermava che:

> *the Contracting States [do not] enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.*[443]

Questa consapevolezza si è tradotta nell'evoluzione giurisprudenziale dell'Art. 8 CEDU, divenuto il primo baluardo del diritto umano alla *privacy* in Europa.[444]

D'altro canto, sul piano legislativo fu percepita la necessità di dettare una disciplina più specifica ed aggiornata. Uno studio promosso dal Comitato dei Ministri nel 1968,[445] dimostrava già all'epoca come l'assetto normativo degli Stati membri non fosse al passo con la crescente automatizzazione delle banche dati.[446] Un comitato di esperti approntò quindi due Risoluzioni, una focalizzata sul settore privato[447] ed una su quello pubblico.[448] Incentivati da queste, diversi paesi[449]

[443] *Klass and others v. Germany* (Application no 5029/71) [1978] CEDU.
[444] *Cfr.* paragrafo precedente.
[445] Lo studio in questione era stato richiesto congiuntamente dall'Assemblea Parlamentare e dal Consiglio d'Europa con la Raccomandazione 509 del 31 Gennaio 1968.
[446] Council of Europe, Explanatory Report – Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108) §1-3.
[447] Consiglio dei Ministri, Risoluzione (73) 22 sulla tutela della riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore privato.

implementarono leggi che riconoscevano, seppur in modo immaturo, diversi principi posti a tutela dei dati personali.[450] Già era stata formulata l'idea di un accordo internazionale vincolante, che potesse uniformare le discipline negli Stati parti ed agevolare il traffico transfrontaliero dei dati.[451] Un nuovo comitato di esperti, specializzato in protezione dei dati personali, elaborò dunque tra il 1976 ed il 1980 il testo di una Convenzione, adottata l'anno successivo dal Comitato dei Ministri.[452]

La Convenzione 108/1981,[453] per la prima volta in maniera esplicita, pone il diritto alla vita privata "in relazione all'elaborazione automatica dei dati a carattere personale".[454] Si tratta di uno strumento fondamentale, che detta i principi ai quali si ispirerà anche il legislatore comunitario.[455]

In primis, vengono fornite definizioni che sono ancora valide per la loro elasticità, sebbene il lessico specifico sia mutato nel corso degli anni. A titolo esemplificativo, i dati a carattere personale sono descritti come "ogni informazione concernente una persona fisica identificata o identificabile («persona interessata»)".[456] Allo stesso modo, può ritenersi ancora valida la definizione di detentore di una collezione di dati:

> la persona fisica o giuridica, la pubblica autorità, il servizio o qualsiasi altro organismo che, secondo la legge nazionale, è competente a decidere quale debba essere la finalità dello schedario automatizzato, quali categorie di dati a carattere personale debbano essere registrate e quali operazioni debbano essere loro applicate.[457]

---

[448] Consiglio dei Ministri, Risoluzione (74) 29 sulla tutela della riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore pubblico.
[449] Council of Europe, Explanatory Report §5.
[450] *Cfr. Ibidem*, §6: "*All national laws recognise: i. the principle of publicity, i.e. that the existence of automated data files should be publicly known; and ii. the principle of control, i.e. that public supervisory authorities as well as the individuals directly concerned by the information can require that the rights and interests of those individuals are respected by the data users.*"
[451] *Ibidem*, 3-4.
[452] *Ibidem*, 4-5.
[453] Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, STE No. 108, 28 Gennaio 1981.
[454] Convenzione 108/1981, Art. 1.
[455] Vd. *infra* Direttiva 95/46/CE.
[456] Convenzione 108/1981, Art. 2(a); *cfr.* Direttiva 95/46/CE, Art. 2(a).
[457] Convenzione 108/1981, Art. 2(d); *cfr.* Direttiva 95/46/CE, Art. 2(d).

Parimenti, le prescrizioni relative alla qualità dei dati sono state poi riprese in larga parte dalla Direttiva 95/46/CE,[458] costruendo un impianto normativo ancora in vigore. Rimandando al paragrafo successivo per un'analisi più approfondita, si può anticipare che i principi in questione sono:[459]

a) Lealtà e legittimità nell'elaborazione automatizzata dei dati;
b) Finalità determinate e legittime. L'utilizzo incompatibile con le finalità dichiarate è vietato;
c) I dati devono essere esatti e sempre aggiornati;
d) Nell'archiviare i dati, l'identificazione dell'interessato deve essere possibile solo per il tempo strettamente necessario al perseguimento dei fini enunciati al momento della registrazione.

Alla voce "garanzie supplementari per la persona interessata"[460] vengono annoverati per la prima volta i diritti sostanziali di cui gode il soggetto in questione: accesso, rettifica, cancellazione e possibilità di ricorso in caso di inerzia del detentore dei dati.[461]

In linea con l'Art. 8 CEDU,[462] è possibile derogare alle disposizioni della Convenzione 108, posto che l'eccezione sia prevista dalla legge nazionale e che la misura sia necessaria "in una società democratica".[463] Inoltre, lo scopo perseguito può essere unicamente la protezione dell'interesse pubblico,[464] della persona interessata o dei diritti di altri individui.[465]

---

[458] Direttiva 95/46/CE, Art. 6.
[459] Vd. Convenzione 108/1981, Art. 5.
[460] Convenzione 108/1981, Art. 8.
[461] Per maggiori dettagli, vd. paragrafo successivo.
[462] Council of Europe, Explanatory Report §55.
[463] Convenzione 108/1981, Art. 9(2).
[464] *Cfr. Ibidem*, §56-57; lo *explanatory report* illustra nel dettaglio la portata della nozione: "*These exceptions are very specific in order to avoid that, with regard to the general application of the convention, States would have an unduly wide leeway. States retain, under Article 16, the possibility to refuse application of the convention in individual cases for important reasons, which include those enumerated in Article 9.*
The notion of "State security" should be understood in the traditional sense of protecting national sovereignty against internal or external threats, including the protection of the international relations of the State.
The term "monetary interests of the State" covers all the different means of financing a State's policies. Accordingly, the term refers in particular to tax collection requirements and exchange control. The term "suppression of criminal offences" in this littera includes the investigation as well as the prosecution of criminal offences."
[465] *Ibidem*, Art. 9(2)(a)(b).

Un altro aspetto essenziale riguarda il trasferimento transfrontaliero di dati. All'Art. 12 è stabilito che le disposizioni fin qui esaminate si applicano anche "ai trasferimenti attraverso i confini nazionali, con qualunque mezzo, di dati a carattere personale oggetto di elaborazione automatica o raccolti allo scopo di sottoporli a tale elaborazione."[466] La formula onnicomprensiva ("con qualunque mezzo") ha una motivazione precisa. Come illustrato nella relazione esplicativa: "*the provisions of Article 12 also apply to data collection. This extension was considered indispensable in order to avoid that data gathered in one country and processed in another would escape the rules set out in this convention.*" Pensando ad un'applicazione pratica di quanto appena riportato, si può pensare che la Convenzione sia invocabile nel caso di attività di SIGINT transfrontaliera (sempre che Stato offensore ed offeso siano entrambi parti della Convezione).

L'Art. 12(2) opera un contemperamento con l'Art. 10 CEDU.[467] Esso vieta limitazioni immotivate al flusso di dati verso altri paesi. In ogni caso è possibile derogare a questo secondo comma qualora i dati siano di natura particolare[468] o per evitare che giungano, anche indirettamente, a Stati terzi che non offrono garanzie idonee.[469]

Si noti che il valore aggiunto della Convenzione, più di ogni altra cosa, sta nel carattere "aperto" dello strumento, che consente la partecipazione di Stati terzi.[470] Una simile opzione non sarebbe stata disponibile se la materia fosse stata regolata unicamente dall'Art. 8 CEDU.[471]

Inquadrando questa risorsa nell'attuale dibattito tra Stati Uniti ed Europa, ciò significa possedere nella Convenzione 108 una possibile soluzione da

---

[466] *Ibidem*, Art. 12(1).
[467] L'Art. 10 concerne la libertà d'espressione, qui intesa come libera circolazione delle informazioni tra gli Stati membri; vd. Council of Europe, Explanatory Report – Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108) §62.
[468] *Ibidem*, Art. 12(3); Council of Europe, Explanatory Report Report §69.
[469] Convenzione 108/1981, Art. 12(3).
[470] Council of Europe, Explanatory Report §24: "*[t]he title describes this instrument as "Convention", not as "European Convention" in order better to underline that there ought to be ample scope for accession to it by non-European States*"; Convenzione 108/1981, Art. 23(1): "[d]opo l'entrata in vigore della presente Convenzione, il Comitato dei Ministri del Consiglio d'Europa potrà invitare qualsiasi Stato non membro del Consiglio d'Europa ad aderire alla presente Convenzione mediante una decisione presa con la maggioranza prevista dall'articolo 20 lettera d dello Statuto del Consiglio d'Europa ed all'unanimità dei rappresentanti degli Stati contraenti aventi diritto di sedere al Comitato."
[471] *Ibidem*, §19.

sottoporre al governo di Washington per risolvere la crisi dei *big data*. Diversi esponenti delle istituzioni europee stanno spingendo in questo senso. Durante il discorso tenutosi il 30 Giugno 2014 a Bonn, il Segretario Generale del Consiglio d'Europa Thorbjørn Jagland proponeva:

> *[o]ur conventions are open to participation from states world-wide. The United States, for example, is a member of our Cybercrime Convention. I therefore invite the US to join forces with Europe again. We can work together to update and reinforce the Data Protection Convention. We can make it become the new global standard. This also makes sense economically. Different rules in the US, EU and elsewhere would almost certainly imply more bureaucracy and higher costs.*[472]

In prospettiva di ciò, è avvertita più che mai l'esigenza di aggiornare la Convenzione 108. Già nel 2012 un comitato *ad hoc* aveva approntato una "proposta di modernizzazione",[473] col fine principale di colmare le lacune che oltre trenta anni di sviluppo informatico avevano creato.[474] Allo stesso modo, la revisione cerca di anticipare le necessità che i futuri progressi tecnologici porteranno nel campo della *privacy* e della tutela dei dati personali.[475] Tra le proposte del comitato consultivo figurano, ad esempio:

1) L'espansione della definizione di dato sensibile. L'Art. 6 è stato arricchito includendo i dati genetici, biometrici e inerenti alla salute della persona.[476]
2) Nuove misure imposte al detentore di dati. Nel trattare dati sensibili devono essere adottate misure adeguate così da evitare di mettere a rischio gli interessi, i diritti e le libertà fondamentali dei soggetti interessati.[477]

---

[472] Secretary General, Speeches, Data Protection, Surveillance and Internet Governance: The Human Rights Perspective. Global Media Forum "From Information to Participation", 30 June 2014; vd. anche Report (2013/2188(INI)) §119: "*[the European parliament] Encourages the US to accede to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), as it acceded to the 2001 Convention on Cybercrime, thus strengthening the shared legal basis between the transatlantic allies*"; vd. European Commission, IP/13/1166, 27 November 2013: "*[t]he U.S. should accede to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), as it acceded to the 2001 Convention on Cybercrime*."

[473] The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS No. 108], Proposition of Modernisation, 18 December 2012.

[474] *Cfr*. M ROTENBERG & D JACOBS, "Updating the Law of Information Privacy: the New Framework of the European Union" (2013) 36 Harv J L & Pub Pol'y 645.

[475] *Ibidem*.

[476] The Consultative Committee, *op. cit.*, Art. 6(1); M ROTENBERG & D JACOBS, *op. cit.* 646.

3) Nuove condizioni per il traffico transfrontaliero di dati. Gli Stati parti possono subordinare il trasferimento al consenso inequivocabile dell'interessato o ad un suo interesse specifico. L'interesse pubblico può sempre prevalere in via eccezionale, ma deve essere "*provided by law and constitute a necessary measure in a democratic society.*"[478]
4) Viene istituita un'autorità di vigilanza, del tutto simile alle autorità garanti previste dalla Direttiva 95/46/CE.[479]

Per completezza, si segnala che i lavori del Consiglio d'Europa in risposta al *datagate* non si esauriscono con la Convenzione 108. Piotr Świtalski, Direttore del *policy planning* del Consiglio, ha sottolineato l'importanza dell'opera giurisprudenziale della CtEDU,[480] unitamente ad altri strumenti normativi e di *soft law*.[481] Tra questi spiccano la Convenzione sul *Cybercrime*, la Risoluzione 1954/2013 (entrambi menzionati *supra*) ed una recente Dichiarazione del Consiglio dei Ministri. Quest'ultima invita gli Stati membri ad implementare legislazioni che regolino l'uso legittimo delle nuove tecnologie di sorveglianza, in modo da tutelare i diritti umani, la democrazia e lo Stato di diritto.[482]

Concludendo, Świtalski propone alcune opzioni alle istituzioni di Strasburgo per guidarle nei mesi futuri.[483] Si tratta di linee guida che riaffermano la necessità di proseguire il dialogo internazionale in materia di *privacy* e di un ammodernamento non solo giuridico, ma anche culturale.[484] In mancanza di

[477] The Consultative Committee, *op. cit.*, Art. 6(2); M ROTENBERG & D JACOBS, *op. cit.* 646.
[478] The Consultative Committee, *op. cit.*, Art. 12(4)(a)(b)(c); M ROTENBERG & D JACOBS, *op. cit.* 646.
[479] The Consultative Committee, *op. cit.*, Art. 12bis; vd. paragrafo successivo.
[480] I *leading cases* in materia sono i succitati *Amann v. Switzerland* e *Leander v. Sweden*; per una rassegna completa, vd. European Court of Human Rights, Research Division, "National security and European case-law" (November 2013).
[481] P ŚWITALSKI, "Snooping on People's Privacy – the Implications of Internet Mass Surveillance on Human Rights" [2013] 11 ALER-T 2.
[482] Council of Europe, Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies (Adopted by the Committee of Ministers on 11 June 2013 at the 1173rd meeting of the Ministers' Deputies).
[483] PIOTR ŚWITALSKI, *op. cit.*: "1) *deepen the internal debate on privacy and mass surveillance and designate a specialised function within the Secretariat to ensure follow-up and activity co-ordination; 2) design a 'privacy and cyberspace' awareness-raising project directed at young people;3) consider the prospect of leading (or alternatively being involved in) the creation of international legally-binding instruments on Internet privacy and mass surveillance; 4) analyse the opportunity to propose a non-aggressive legal mechanism on Internet-tracing together with a verification process; 5) propose the inclusion of data processing education on schools' curricula and develop relevant public campaigns.*"
[484] *Ibidem*.

rimedi giurisdizionali o misure di *follow up*, allo stato attuale non c'è altro modo per consentire un impatto reale su di un fenomeno così complesso.[485]

2.2.3. La Direttiva 95/46/CE

Lo sforzo del Consiglio d'Europa nel 1981 fu recepito e assecondato dal legislatore della Comunità (oggi Unione) Europea. Con l'entrata in vigore del Trattato di Maastricht, nel 1992, le istituzioni europee avevano già intrapreso un percorso che le ha portate gradualmente a svincolarsi da interessi puramente economici.[486] La Direttiva 95/46/CE[487] si colloca in questo particolare momento di transizione e ne risente, mostrando infatti un obiettivo duplice.[488] Da un lato ancora si preoccupa di promuovere il mercato interno, impostando standard comuni per il trasferimento dei dati. Dall'altro si prefigge di tutelare un diritto fondamentale dell'individuo: [489] quello alla "vita privata, con riguardo al trattamento dei dati personali".[490] Come già asserito, la Direttiva pone le proprie basi sulle previsioni dell'Art. 8 CEDU e della Convenzione 108/1981.[491]

Per estendere quanto più possibile la protezione garantita, vengono adottate definizioni ampie dei diversi termini-chiave.[492] I dati personali sono descritti come "qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata»); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale". [493] Il trattamento dei dati personali consiste invece in "qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione,

---

[485] *Ibidem*.
[486] S SIMITIS, "From the Market to the Polis: The EU Directive on the Protection of Personal Data" [1995] 80 Iowa L Rev 447-448; M ROTENBERG & D JACOBS, *op. cit.* 616.
[487] Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati.
[488] RUSSO S., *op. cit.* 12; M ROTENBERG & D JACOBS, *op. cit.* 617.
[489] Direttiva 95/46/CE Considerando 10.
[490] *Ibidem*, Art. 1(1).
[491] *Cfr. supra;* Direttiva 46/95/CE Considerando 8, 11.
[492] M ROTENBERG & D JACOBS, *op. cit.* 617.
[493] Direttiva 95/46/CE, Art. 2(a).

l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione".[494]

Gli Stati Membri sono chiamati ad implementare leggi che dispongano un trattamento lecito e leale.[495] Da questi due principi discende una serie di altri canoni indefettibili. Innanzitutto, le informazioni devono essere sempre esatte ed aggiornate. [496] Nel conservarle, deve essere consentita l'identificazione dell'interessato[497] solo per il tempo strettamente necessario al conseguimento delle finalità del trattamento.[498] Quest'ultimo deve essere svolto nella massima riservatezza[499] e sicurezza.[500]

La Direttiva mette a disposizione del soggetto interessato anche dei diritti sostanziali i.e. accesso e rettifica.[501] Il primo consente di apprendere in ogni momento se esista o meno un trattamento presso il responsabile. Qualora i dati non risultassero conformi, è possibile imporre che siano rettificati, cancellati o congelati.[502]

Come regola generale, l'interessato deve aver prestato il proprio consenso inequivocabile, ma sono possibili delle eccezioni.[503] Tra queste, le più rilevanti si ricollegano alla presenza di un interesse pubblico o all'esercizio dei pubblici poteri. [504] Dal testo normativo emerge che sono ammesse deroghe quando necessario i.a. per la salvaguardia della sicurezza dello Stato, della difesa o della pubblica sicurezza.[505] Cionondimeno, la Corte di Giustizia ha specificato in più di un'occasione che l'applicazione della Direttiva nella sua interezza deve essere la

[494] *Ibidem*, Art. 2(b).
[495] *Ibidem*, Art. 6(1).
[496] *Ibidem*, Art. 6(1)(d).
[497] Per "soggetto interessato" si intende la persona cui i dati trattati si riferiscono.
[498] Direttiva 95/46/CE, Art. 6(1)(e).
[499] *Ibidem*, Art. 16.
[500] *Ibidem*, Art. 17.
[501] *Ibidem*, Art. 12.
[502] M ROTENBERG & D JACOBS, *op. cit.* 619.
[503] *Ibidem*, Art. 7.
[504] *Ibidem*, Art. 7(e).
[505] *Ibidem*, Art. 13(1)(a)(b)(c).

norma, mentre le disposizioni derogatorie sono eccezionali e vanno interpretate restrittivamente.[506]

Nel caso *Österreichischer Rundfunk* [507] la CGUE evidenziò l'importanza degli Artt. 6 e 7 della Direttiva, che subordinano il trattamento nell'interesse pubblico (esattamente come ogni altro) ai principi di adeguatezza, pertinenza, non eccedenza[508] e necessità.[509] Tali presupposti, proseguiva la Corte, devono essere letti alla luce dell'Art. 8(2) CEDU.[510] Una simile affermazione non giunge completamente inaspettata, se si tiene conto del processo di interazione tra gli ordinamenti UE e CEDU avviato dal trattato di Maastricht e di cui si faceva menzione *supra*.[511]

Si deve considerare anche il contributo apportato, in quello stesso periodo (l'anno è il 2000), dalla Carta di Nizza.[512] Questa all'Art. 53 stabilisce che "[n]essuna disposizione della presente Carta deve essere interpretata come limitativa o lesiva dei diritti dell'uomo e delle libertà fondamentali riconosciuti […] dalle convenzioni internazionali delle quali l'Unione, la Comunità o tutti gli Stati membri sono parti contraenti, in particolare la convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali".

Fondando l'interpretazione di una Direttiva comunitaria sull'Art. 8 CEDU, la CGUE ha di fatto imposto un doppio standard nel diritto alla tutela dei dati personali. Per questo motivo si potrebbe ravvisare nel caso *Österreichischer Rundfunk* un'anticipazione della sentenza *Bosphorus*,[513] ricognitiva del principio della cd. "protezione equivalente". Ad ogni modo, è innegabile è che la Direttiva 95/46/CE sia fortemente legata alla tutela dei dati personali come diritto

---

[506] P DE HERT, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action" (2009) Springer Science 20.
[507] CGUE, *Österreichischer Rundfunk*, sentenza 20 Maggio 2003, cause riunite C-465/00, C-138/01 e C-139/01.
[508] Direttiva 95/46/CE, Art. 6(c).
[509] *Ibidem*, Art. 7(e); vd. *Österreichischer Rundfunk* Cause riunite C-465/00, C-138/01, C-139/01 §66-72; *cfr.* P DE HERT, *op. cit.* 21.
[510] "Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale […]"; vd. più approfonditamente *infra*.
[511] Trattato sull'Unione Europea 191/01 (92/C), Art. F(2); *cfr.* Versione Consolidata del Trattato sull'Unione Europea C/321 (E/1), Art. 6(2).
[512] Carta dei Diritti Fondamentali dell'Unione Europea 364/1 (2000/C); *cfr.* P DE HERT, *op. cit.* 21.
[513] *Bosphorus Hava Yollari Turizm ve Ticaret Anonim Şirketi v. Ireland* (Application no 45036/98) [2005] CEDU.

umano.[514] Ciò significa garantire alti standard di protezione all'individuo, lasciando in secondo piano altre finalità prettamente economiche.[515]

2.2.4. La nuova proposta di Regolamento

La Direttiva 95/46/CE è stata giustamente definita una "pietra angolare nell'impianto della vigente normativa dell'UE in materia di protezione dei dati personali".[516] Ciononostante, il progresso informatico ha generato rapidamente nuove esigenze e nuovi problemi da risolvere.[517] La diffusione del Web, ampliatasi in modo esponenziale, ha reso insufficienti le tutele attuali. L'uso quotidiano dei *social media*, fra tutti, rende ormai lacunose le garanzie offerte dai diritti d'accesso e di rettifica, considerata la mole straordinaria di dati (anche sensibili) che vengono diffusi in rete ogni giorno.[518]

Un altro difetto noto della Direttiva risiede nell'Art. 25(1).[519] Questo consente il trasferimento di dati verso paesi terzi che garantiscano un "livello di protezione adeguato". Tuttavia, manca una definizione chiara ed esaustiva di "adeguatezza",[520] lasciando che la valutazione sia compiuta dagli Stati Membri e della Commissione senza criteri specifici.[521]

Ancora, la normativa in vigore manca di regolare le conseguenze di eventuali furti di dati.[522] Esiste un correttivo nel testo della Direttiva

---

[514] P DE HERT, *op. cit.* 21.
[515] *Cfr.* CGUE, *Lindqvist*, sentenza 6 Novembre 2003, C101-01.
[516] Relazione COM(2012) 11 final §1.
[517] M ROTENBERG & D JACOBS, *op. cit.* 623.
[518] *Ibidem*, 624; *cfr.* Relazione COM(2012) 11 final §1.
[519] "Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva."
[520] Direttiva 95/46/CE, Art. 25(2): "L'adeguatezza del livello di protezione garantito da un paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate"; *cfr.* M ROTENBERG & D JACOBS, *op. cit.* 626.
[521] *Ibidem*, Art. 25(3): "Gli Stati membri e la Commissione si comunicano a vicenda i casi in cui, a loro parere, un paese terzo non garantisce un livello di protezione adeguato ai sensi del paragrafo 2"; *cfr.* M ROTENBERG & D JACOBS, *op. cit.* 626.
[522] Si tratta di una realtà che interessa centinaia di milioni di dati. Vd. Verizon Enterprise Solutions, "Verizon Data Breach Investigation Report" [2014]: http://www.verizonenterprise.com/it/DBIR/2014/; M ROTENBERG & D JACOBS, *op. cit.* 625.

2002/58/CE.[523] L'Art. 4(2) recita: "[n]el caso in cui esista un particolare rischio di violazione della sicurezza della rete, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha l'obbligo di informarne gli abbonati indicando, qualora il rischio sia al di fuori del campo di applicazione delle misure che devono essere prese dal fornitore di servizio, tutti i possibili rimedi, compresi i relativi costi presumibili". La disposizione in esame, però, risolve solo parzialmente il problema. Infatti, la sua portata oggettiva è limitata ai "servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nella Comunità".[524]

L'insieme di queste concause ha portato la Commissione a presentare una proposta di Regolamento Generale sulla Protezione dei Dati.[525] Il cd. RGPD, forte dell'Art. 16 del Trattato di Lisbona,[526] si prefigge l'obiettivo di "creare un quadro globale per la protezione dei dati, che copra tutti i settori".[527] Sviluppando la formula d'ampio respiro presente nella Direttiva attuale, il Regolamento tutela quale soggetto interessato "la persona fisica identificata o identificabile, direttamente o indirettamente, con mezzi che il responsabile del trattamento o altra persona fisica o giuridica ragionevolmente può utilizzare, con particolare riferimento a un numero di identificazione, a dati relativi all'ubicazione, a un identificativo on line o a uno o più elementi caratteristici della sua identità genetica, fisica, fisiologica, psichica, economica, culturale o sociale". Già in apertura, il RGPD mostra una sensibilità nuova verso categorie di dati (si notino i.a. quelli genetici) che per ragioni cronologiche erano stati tralasciati dalla Direttiva.[528]

---

[523] Direttiva 2002/58/CE del 12 Luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.
[524] Direttiva 2002/58/CE, Art. 3(1).
[525] Proposta di Regolamento del Parlamento Europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, [2012] Bruxelles COM 2012.
[526] *Ibidem*, Considerando 10; vd. TFUE Art.16(2): "Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti."
[527] Relazione COM(2012) 11 final, Scheda finanziaria legislativa §1.4.1.
[528] M ROTENBERG & D JACOBS, *op. cit.* 631.

Seguendo la medesima *ratio*, il Regolamento ha cura di specificare che indirizzi IP, marcatori temporanei[529] ed altri identificativi online possono essere considerati dati personali, a seconda delle circostanze. Ciò è vero se si considera che tali informazioni, quando combinate con altri identificativi univoci o dati ottenuti dai server, possono essere sfruttate per identificare un utente specifico.[530]

La prima novità sostanziale del RGPD è stata introdotta all'Art. 7(1), il quale statuisce che "[l]'onere di dimostrare che l'interessato ha espresso il consenso al trattamento dei suoi dati personali per scopi specifici incombe sul responsabile del trattamento". Con questa inversione dell'onere della prova, si alleggerisce ulteriormente il carico degli obblighi dell'interessato, confermando la tendenza generale del Regolamento a favorire il diritto alla *privacy* dei cittadini.

In modo altrettanto significativo, vengono potenziate le disposizioni relative al cd. "consenso informato".[531] Non solo il consenso deve essere esplicito e basato su un'informativa trasparente e completa,[532] ma deve altresì essere necessariamente espresso in forma scritta.[533] Il consenso implicito non è più previsto come base legale per il trattamento.[534]

Infine, sono state aggiunte altre previsioni volte a garantire la persistenza e la genuinità del consenso prestato: quest'ultimo non è valido qualora vi sia un "notevole squilibrio tra la posizione dell'interessato e del responsabile del trattamento",[535]ed in ogni caso "[l]' interessato ha il diritto di revocare il proprio consenso in qualsiasi momento"[536] senza pregiudizio del trattamento lecitamente svolto in precedenza.

Sul piano dei diritti sostanziali, viene riconosciuto in modo esplicito il "diritto all'oblio".[537] L'Art. 17(1) recita:

---

[529] Meglio noti con il nome di *cookies*.
[530] RGPD, Considerando 24.
[531] *Cfr*. Direttiva 95/46/CE, Considerando 30, Art. 7.
[532] *Cfr*. RGPD, Art. 11: "Il responsabile del trattamento fornisce all'interessato tutte le informazioni e le comunicazioni relative al trattamento dei dati personali in forma intelligibile, con linguaggio semplice e chiaro e adeguato all'interessato, in particolare se le informazioni sono destinate ai minori."
[533] *Ibidem*, Art. 7(2).
[534] M ROTENBERG & D JACOBS, *op. cit.* 632.
[535] RGPD, Art. 7(4).
[536] *Ibidem*, Art. 7(3).
[537] M ROTENBERG & D JACOBS, *op. cit.* 632.

> [l]'interessato ha il diritto di ottenere dal responsabile del trattamento la cancellazione di dati personali che lo riguardano e la rinuncia a un'ulteriore diffusione di tali dati, in particolare in relazione ai dati personali resi pubblici quando l'interessato era un minore […]

L'articolo in parola attualizza forse nel modo più fedele il "*right to be let alone*" teorizzato da BRANDEIS e WARREN.[538]

In verità, la giurisprudenza della CGUE già si è mossa nel senso di riconoscere un diritto all'oblio in capo ai cittadini dell'Unione. Con la sentenza *Google Spain*,[539] la Grande Sezione riconosce già in forza della Direttiva 95/46/CE, Artt. 12(b) e 14(1)(a) che:

> il gestore di un motore di ricerca è obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine web sia di per sé lecita.[540]

In questa parte del dispositivo si ritrova il principale aspetto del diritto all'oblio, che consiste nella cancellazione di tutti i dati riguardanti uno stesso interessato che ne faccia richiesta.[541] Sulla base dei medesimi articoli, la Corte riconosce anche un'ulteriore facoltà all'interessato dal trattamento, ovverosia che:

> la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome, senza per questo che la constatazione di un diritto siffatto presupponga che l'inclusione dell'informazione in questione in tale elenco arrechi un pregiudizio a detto interessato. Dato che l'interessato può, sulla scorta dei suoi diritti fondamentali derivanti dagli articoli 7 e 8 della Carta, chiedere che l'informazione in questione non venga più messa a

[538] I due autori statunitensi, con il loro celebre articolo, ponevano le basi per lo sviluppo della disciplina odierna in materia di *privacy*; *cfr.* L BRANDEIS & S D WARREN, "The Right to Privacy" [1890] 4 Harvard L Rev 193.
[539] CGUE, *Google Spain SL / Google Inc. v. Agencia de Protección de Datos(AEPD), Mario Costeja González*, sentenza 13 Maggio 2014, C-131/12.
[540] *Ibidem*.
[541] *Cfr.* RGPD, Art. 17(2).

> disposizione del grande pubblico in virtù della sua inclusione in un siffatto elenco di risultati, i diritti fondamentali di cui sopra prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico ad accedere all'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, in virtù dell'inclusione summenzionata, all'informazione di cui trattasi.[542]

Questa seconda asserzione della Corte descrive il cd. "diritto ad essere lasciati in pace". Inoltre, sono riconfermati molti dei principi affrontati *supra*: quelli sanciti dalla Carta di Nizza, la predilezione per la *privacy* nel contemperamento con altri diritti, la prevalenza dell'interesse pubblico solo in casi eccezionali.

A seguito della sentenza, Google Inc. ha prontamente messo a disposizione dei suoi utenti una pagina web contenente un modulo per richiedere la rimozione dei risultati di ricerca.[543] Un'operazione del genere, essendo stata promossa da una delle imprese leader nel settore, ha sicuramente un peso notevole. Resta solo da appurare in che modo, nei prossimi mesi, i prestatori di servizi concorrenti si adegueranno al dettato della Grande Sezione.

Tornando all'analisi del RGPD, un nuovo aspetto da esaminare riguarda la tutela prevista contro eventuali violazioni dei dati personali, che come si è detto costituisce una lacuna importante nell'attuale disciplina. L'Art. 31(1) prescrive che:

> [i]n caso di violazione dei dati personali, il responsabile del trattamento notifica la violazione all'autorità di controllo senza ritardo, ove possibile entro 24 ore dal momento in cui ne è venuto a conoscenza. Qualora non sia

[542] CGUE, *Google Spain SL / Google Inc. v. Agencia de Protección de Datos (AEPD), Mario Costeja González*, sentenza 13 Maggio 2014, C-131/12.
[543] https://support.google.com/legal/contact/lr_eudpa?product=websearch.

effettuata entro 24 ore, la notificazione all'autorità di controllo è corredata di una giustificazione motivata.[544]

È inoltre previsto che sia informato anche l'interessato, se ne può derivare pregiudizio alla sua vita privata o ai dati stessi.[545] Se il responsabile non dimostra di aver adottato "le opportune misure tecnologiche di protezione" e che tali misure "erano state applicate ai dati violati",[546] la comunicazione è sempre imposta dall'autorità di controllo.[547] In generale, si richiede "l'attuazione di adeguate misure tecniche e organizzative al momento sia della progettazione che dell'esecuzione del trattamento stesso", [548] al fine di realizzare la cd. "protezione fin dalla progettazione".[549]

Infine, si segnala la previsione dei nuovi mezzi di ricorso di cui al Capo VIII del RGPD. Innanzitutto, l'Art. 73 prevede la possibilità di presentare un reclamo all'autorità di controllo per lamentare presunte violazioni del Regolamento.[550] In secondo luogo, "ogni persona fisica o giuridica" [551] ha diritto al ricorso giurisdizionale tanto per riformare la decisione pronunciata all'esito del reclamo, quanto per obbligare l'autorità (se rimasta inerte) a dare seguito al reclamo stesso.[552] Salvo cause di esclusione della responsabilità, qualora sia effettivamente riscontrata una violazione del Regolamento l'Art. 77(1) prevede "il diritto di ottenere il risarcimento del danno dal responsabile del trattamento o dall'incaricato del trattamento." Le sanzioni amministrative già disposte dalla Direttiva 95/46/CE sono riconfermate nel dettato degli Artt. 78 e 79.

2.2.4. Continua: l'efficacia transnazionale del RGPD

[544] Nella notificazione sono indicate l'entità e le conseguenze della violazione, le misure adottate e quelle proposte per porvi rimedio, nonché l'identità del responsabile della protezione dei dati; *cfr.* RGPD, Art. 31(3).
[545] *Ibidem*, Art. 32(1).
[546] RGPD, Art. 32(3).
[547] *Ibidem*, Art. 32(4).
[548] *Ibidem*, Considerando 61.
[549] *Ibidem*; *cfr. Ibidem*, Art. 23(1).
[550] Vd. anche l'Art. 73(2), che prevede la possibilità di proporre il reclamo da parte di organismi, organizzazioni o associazioni che tutelino "i diritti e gli interessi degli interessati in relazione alla protezione dei loro dati personali e che [siano debitamente costituite] secondo la legislazione di uno Stato membro".
[551] *Ibidem*, Art. 74(1).
[552] *Ibidem*, Art. 74(2).

Il vantaggio più evidente nell'implementazione di un Regolamento in materia di *privacy* e tutela dei dati personali sarebbe ovviamente nel superiore grado di armonizzazione garantito dal tipo di strumento normativo. Infatti, si rammenta che ex Art. 288(2) TFUE il Regolamento "ha portata generale. Esso è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri". La Direttiva 95/46/CE, che nell'opinione della CGUE persegue un obiettivo di "armonizzazione totale",[553] ha ravvicinato di molto le legislazioni degli Stati membri, ma i risultati ottenuti non sono sempre identici né di facile coordinamento.[554] Come sostenuto dallo stesso HUSTINX, Garante europeo della protezione dei dati, "*we now have ended up with 27 different versions of the same basic principles. This is simply too much, and translates into costs, but also a loss of effectiveness. In other words, there is a need to scale up harmonization*".[555]

In vista di un simile traguardo, il RGPD prevede un "meccanismo di coerenza"[556] che coinvolge direttamente le autorità di controllo istituite nei vari Stati membri. Queste, insieme con la Commissione, sono tenute a cooperare nello svolgimento delle funzioni di cui all'Art. 46(1).[557] Concretamente, ciò si traduce nell'obbligo imposto alle autorità di controllo di sottoporre ogni progetto di misura in procinto di essere adottata[558] al Comitato europeo per la protezione dei dati[559] e alla Commissione.[560] Questi a loro volta possono esprimere pareri,[561]

[553] P DE HERT, *op. cit.* 20; Y POULLET; "EU Data Protection Policy, the Directive 95/46/CE: Ten Years After" [2006] Computer Law & Security Report 206-217.
[554] P HUSTINX, "High Level Conference: "Ethical Dimensions of Data Protection and Privacy" Centre for Ethics, University of Tartu / Data Protection Inspectorate" (2013) European Data Protection Supervisor.
[555] *Ibidem*.
[556] RGPD, Art. 57.
[557] "Ogni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare l'applicazione del presente regolamento e di contribuire alla sua coerente applicazione in tutta l'Unione, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali e di agevolare la libera circolazione dei dati personali all'interno dell'Unione. A tale scopo le autorità di controllo cooperano tra loro e con la Commissione."
[558] Per "misura" si intende, ex Art. 58(2) RGPD, qualsiasi provvedimento che influenzi più di uno Stato membro. Ad esempio, l'articolo annovera i.a. misure concernenti "attività di trattamento finalizzate all'offerta di beni o servizi a interessati in più Stati membri", oppure che possano "incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione".
[559] Il comitato europeo per la protezione dei dati è un organo composto ex Art. 64 RGPD "dal responsabile di un'autorità di controllo di ciascuno Stato membro e dal garante europeo della protezione dei dati", la cui funzione è (ex Art. 66) quella di garantire "l'applicazione coerente" del Regolamento.
[560] *Cfr.* RGPD, Art. 58(1).
[561] *Ibidem*, Art. 59.

sospendere i progetti[562] o persino avviare una procedura d'urgenza[563] in casi eccezionali che richiedono l'adozione di misure provvisorie.[564]

Per ciò che riguarda l'applicabilità del Regolamento ai paesi terzi, la nuova disciplina è più dettagliata rispetto a quella vigente. La materia è sviluppata nel Capo V del RGDP, rubricato "trasferimento di dati personali verso paesi terzi o organizzazioni internazionali". In generale, è stato mantenuto il preesistente criterio dell'adeguatezza, in assenza del quale non è possibile il trasferimento.[565] La valutazione in merito, però, è accentrata nelle mani della Commissione, in modo da garantire maggiore uniformità.[566] È stato altresì arricchito l'elenco degli elementi che la Commissione deve prendere in esame per poter raggiungere una decisione.[567] Tra questi, spiccano lo stato della legislazione vigente in materia di pubblica sicurezza, difesa e sicurezza nazionale (nota dolente nell'ordinamento giuridico statunitense), l'esistenza di autorità di controllo e l'azionabilità di ricorsi amministrativi o giudiziari.[568] Nel silenzio della Commissione il trasferimento è possibile, purché siano prestate "garanzie adeguate" ex Art. 42(2).[569] Parimenti, resta possibile l'applicazione di deroghe alle regole appena enunciate,[570] ma con diverse limitazioni.[571]

2.3. Trasferimenti di dati tra USA e UE: l'accordo *Safe Harbor*

In attesa dell'entrata in vigore del RGPD, i trasferimenti di dati verso paesi terzi rimangono soggetti al disposto degli Artt. 25 e 26 della Direttiva 95/46/CE. Limitatamente ai trasferimenti tra Stati Uniti ed Unione Europea, già dal 2000 la

[562] *Ibidem*, Art. 60.
[563] *Ibidem*, Art. 61.
[564] *Cfr.* M ROTENBERG & D JACOBS, *op. cit.* 636.
[565] RGPD, Art. 41(1).
[566] *Ibidem*.
[567] *Ibidem*, 41(2).
[568] *Ibidem*.
[569] Si tratta di un elenco aperto, dal momento che ex Art. 42(2)(d) il responsabile del trattamento può sempre richiedere un'autorizzazione preventiva all'autorità di controllo di appartenenza. È prevista anche l'attivazione del meccanismo di coerenza descritto *supra* nel caso in cui il trasferimento coinvolga più di uno Stato membro ed almeno un paese terzo.
[570] *Cfr.* Direttiva 95/46/CE, Art. 26; RGPD, Art. 44.
[571] Tra le varie condizioni per derogare, si evidenziano i "motivi d'interesse pubblico generale" ex Art. 44(1)(d). Riconfermando ancora una volta l'approccio garantista dell'Unione in materia di dati personali, l'Art. 44(7) specifica che alla Commissione è conferito il potere di precisare in cosa effettivamente consistano tali motivi di interesse pubblico, attraverso un atto delegato ex Art. 86.

Commissione aveva tentato con un'apposita Decisione[572] di adeguare gli standard degli Stati Uniti ai dettami della Direttiva. In quella sede, è stata riconosciuta l'adeguatezza ex Art. 25(2) di tutte quelle "organizzazioni aventi sede negli Stati Uniti"[573] uniformatesi ai "principi di approdo sicuro in materia di riservatezza" (denominati *safe harbour principles*[574] nella direttiva del Dipartimento del commercio USA).

La qualifica è puramente volontaria[575] e può essere ottenuta tanto tramite autocertificazione, quanto a seguito di una valutazione effettuata da terze parti.[576] Le organizzazioni interessate si impegnano a rispettare una serie di parametri che abbracciano diversi aspetti:

- Notifica: i soggetti interessati dal trattamento devono essere informati del fatto che i propri dati sono stati raccolti e di come saranno trattati.[577]
- Scelta: ai soggetti interessati deve essere concessa la cd. "facoltà di rifiuto", ovverosia di impedire l'ulteriore trattamento o trasferimento a terzi dei dati.[578]
- Trasferimento successivo: in questo caso, anche i terzi riceventi devono adeguarsi ai principi dell'approdo sicuro. Possono alternativamente garantire, con un accordo *ad hoc*, che sarà fornito un livello di protezione pari o superiore.[579]
- Sicurezza: consiste nel "prendere ragionevoli precauzioni per [proteggere le informazioni personali] da perdita ed abusi nonché da accesso, rivelazione, alterazione e distruzione non autorizzati."[580]

[572] 2000/250/CE: Decisione della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti".
[573] *Ibidem*, Art. 1.
[574] *Ibidem*, Allegato I; US Department of Commerce [2000] OJ L 215/7; vd. anche il sito ufficiale del Governo USA: http://www.export.gov/safeharbor/eu/eg_main_018365.asp.
[575] Decisione 2000/250/CE, Allegato I.
[576] *Ibidem*, Allegato II, FAQ 6; *cfr.* M ROTENBERG & D JACOBS, *op. cit.* 638.
[577] Decisione 2000/250/CE, Allegato I; M ROTENBERG & D JACOBS, *op. cit.* 638.
[578] *Ibidem*.
[579] *Ibidem*.
[580] *Ibidem*.

- Integrità dei dati: "un'organizzazione deve prendere provvedimenti ragionevoli per garantire che i dati siano attendibili in funzione dell'uso che si prevede di farne, accurati, completi e aggiornati."[581]
- Accesso: esattamente come prescritto dalla Direttiva 95/46/CE, è il diritto dell'interessato ad accedere alle informazioni che lo riguardano e contestualmente correggerle, emendarle o cancellarle quando inesatte.[582]
- Garanzie d'applicazione: si tratta della predisposizione di "meccanismi volti a garantire il rispetto dei principi, la possibilità di ricorso per gli individui cui si riferiscono i dati che vedano lesi i propri interessi dal mancato rispetto dei principi stessi, e la non impunità di un'organizzazione che non rispetti i principi".[583] È stato approntato un sistema di verifica che attesta la sussistenza dei requisiti di autocertificazione ogni dodici mesi.[584] Nel caso in cui siano riscontrate delle difformità, è stabilito che "[l]e dichiarazioni ingannevoli rese al Dipartimento del commercio (od alla persona fisica o giuridica da esso designata) sono perseguibili in forza della legge sulle false dichiarazioni (*False Statements Act*, 18 U.S.C. § 1001)."[585]

Si deve ammettere che agli sforzi della Commissione e del Dipartimento del commercio non hanno fatto seguito risultati soddisfacenti.[586] Soltanto due anni dopo l'entrata in vigore dell'accordo *Safe Harbor*, un rapporto della Commissione individuava seri problemi in merito all'effettiva applicazione dello stesso.[587]

> *A substantial number of organisations that have self-certified adherence to the Safe Harbour do not seem to be observing the expected degree of transparency as regards their overall commitment or as regards the contents of their privacy policies.*[588]

---

[581] *Ibidem*.
[582] *Ibidem*.
[583] *Ibidem*.
[584] Decisione 2000/250/CE, Allegato II, FAQ 6; M ROTENBERG & D JACOBS, *op. cit.* 639.
[585] *Ibidem*.
[586] M ROTENBERG & D JACOBS, *op. cit.* 639.
[587] Commission Staff Working Paper: The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, SEC [2002] 196.
[588] *Ibidem*, 2.

La stessa scarsa efficacia affliggeva le sanzioni previste in caso di non ottemperanza:

> *not all dispute resolution mechanisms have indicated publicly their intention to enforce Safe Harbour rules and not all have in place privacy practices applicable to themselves that are in conformity with the Principles, as required by Safe Harbour rules.*[589]

Un secondo studio condotto nel 2004, su un campione pari al 10% delle organizzazioni certificate, non faceva altro che confermare le problematiche note:[590]

> *[t]he Commission services are concerned that relatively few organisations published privacy policies that reflect all seven Safe Harbour Principles and believe that this problem must be overcome.*[591]

La Commissione richiamava dunque l'attenzione delle autorità statunitensi, affinché compissero sforzi concreti per guidare e monitorare le società aderenti al programma.[592]

Il passo compiuto dal *Department of Commerce* in questo senso, risale solo al 2011, quando fu raggiunto un accordo tra la *Federal Trade Commission* e Google Inc., accusata di aver violato la *privacy* dei propri utenti (i.a. europei) con il lancio di un nuovo *social network*: "Google Buzz".[593] Questo canale informatico, aperto nel 2010, rendeva di fatto impossibile la rimozione o il controllo dei contenuti condivisi, a causa di un'interfaccia caotica e di difficile utilizzo. La società americana fu dunque chiamata ad uniformarsi ai principi *Safe Harbor*, ma nessuna sanzione fu applicata.[594]

---

[589] *Ibidem*.
[590] Commission Staff Working Paper: The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, SEC [2004] 1323; M ROTENBERG & D JACOBS, *op. cit.* 639.
[591] Commission Staff Working Paper, SEC [2004] 1323, 8.
[592] *Ibidem*.
[593] Vd. http://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; M ROTENBERG & D JACOBS, *op. cit.* 640.
[594] *Ibidem*.

Purtroppo, non esistono altri casi degni di nota. Nel successivo rapporto del 27 Novembre 2013,[595] è stato illustrato come tutte le inadeguatezze affiorate nei precedenti quattordici anni fossero ancora persistenti.[596] Le rivelazioni in merito alle attività di sorveglianza delle agenzie americane di *intelligence* non hanno fatto altro che accrescere le preoccupazioni della Commissione e degli Stati membri.[597] Il 24 Luglio 2013 l'Autorità Garante della Germania, prima fra tutte, denunciava la grave minaccia costituita dalle operazioni della NSA per il traffico di dati transfrontaliero.[598] Altri Garanti al contrario, almeno in un primo momento, hanno ritenuto di non dover compiere indagini più approfondite.[599] Nell'opinione della Commissione, tale disomogeneità nelle reazioni delle autorità di controllo non fa che aggravare ulteriormente la frammentazione della cornice *Safe Harbor*, diminuendo gravemente la fiducia in questo strumento.

Attualmente, la crisi nei trasferimenti di dati USA-UE prosegue. Viviane Reding, già Commissario europeo per la Giustizia, i Diritti fondamentali e la Cittadinanza,[600] ha tenuto un discorso in proposito il 28 Gennaio 2014.[601] Nel pieno della discussione accesa dallo scandalo *datagate*, la Reding sosteneva chiaramente la necessità di rafforzare le garanzie di sicurezza offerte dall'approdo sicuro, promuovendo tredici punti sviluppati dalla Commissione.[602] Oltre ad appellarsi nuovamente al *Department of Commerce*, demandando un controllo più stringente sulle società autocertificate, sono state auspicate procedure di *follow-up* nei confronti dei trasgressori ed un ricorso maggiore a sistemi stragiudiziali di

[595] European Commission, Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final.
[596] *Ibidem*, 5.
[597] *Ibidem*.
[598] *Ibidem*; vd. http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870.
[599] I.a. Irlanda e Lussemburgo. La *High Court* irlandese, tuttavia, ha accettato di sottoporre a scrutinio l'inerzia dell'Autorità Garante; vd. COM(2013) 847 final 5.
[600] Nonché vice-presidente della Commissione fino al 1° Luglio 2014. Attualmente è membro del Parlamento europeo. Vd. http://ec.europa.eu/commission_2010-2014/reding/index_en.htm.
[601] European Commission, SPEECH/14/62, 28 January 2014.
[602] *Ibidem*, 3; per la lista completa vd. European Commission, MEMO/13/1059, 27 November 2013, 4.

risoluzione delle dispute.[603] La raccomandazione più rilevante, certamente influenzata dalla vicenda Snowden, è la tredicesima:

> *[i]t is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly* necessary *or* proportionate[604] (enfasi aggiunta).

Ancora una volta, i principi comunitari di proporzionalità e necessità si scontrano con l'ordinamento americano, che predilige la ragion di Stato a scapito delle libertà civili. Se il Governo USA rimarrà ancora inerte ed il *Safe Harbor* non sarà rafforzato, prosegue il Commissario europeo, la Commissione è pronta a sospendere l'accordo.

Da ultimo, il rapporto del comitato LIBE del Parlamento europeo[605] condivide le perplessità espresse sull'approdo sicuro alla luce dell'attività di sorveglianza della NSA.[606] In particolare viene evidenziato come le società al centro delle rivelazioni di Snowden (i.a. Google, Microsoft, Yahoo!, Facebook, Apple e LinkedIn) fossero tutte autocertificate in forza del *Safe Harbor Agreement*.[607] In ragione di ciò, è stata consigliata alla Commissione la sospensione immediata della Decisione 2000/250/CE.[608] Si richiede altresì l'interruzione del traffico di dati verso qualsiasi organizzazione aderente al *Safe Harbor*, salvo il ricorso ad altri strumenti più sicuri.[609]

2.4. La normativa USA

2.4.1. Evoluzione giurisprudenziale del IV emendamento

Il quarto emendamento alla costituzione degli Stati Uniti d'America fu introdotto nel 1789 come parte del *Bill of Rights*: un corpus di dieci emendamenti, tutti volti a limitare il potere del governo federale.

Rubricato "*search and seizure*", questo dispone che:

---

[603] European Commission, MEMO/13/1059, 4.
[604] *Ibidem*.
[605] European Parliament, Report (2013/2188(INI)).
[606] *Ibidem*, Considerando AF-AI, §35-41.
[607] *Ibidem*, §35.
[608] *Ibidem*, §39.
[609] *Ibidem*, §40.

> *[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*[610]

In questa sede saranno mostrate le complesse interrelazioni che legano tale norma con l'attività di sorveglianza domestica e di *intelligence* in senso lato.

Al contrario di quanto si possa pensare, le indagini per la sicurezza nazionale[611] non nascono all'indomani dell'11 Settembre 2011, ma fanno parte di un *leitmotiv* che accompagna gli Stati Uniti sin dalla sua indipendenza. Esistono persino testimonianze di agenti ingaggiati nel 1797 dal Segretario di Stato Timothy Pickering per indagare su possibili accordi sediziosi tra la marina britannica ed il senatore americano William Blount.[612]

La prima preoccupazione, condivisa tanto dalle agenzie federali quanto dalla giurisprudenza, è stata quella di giustificare la legittimità dei propri mezzi di intercettazione o di sorveglianza comunque intesa.[613]

In particolare, durante l'amministrazione di Franklin Roosevelt,[614] ebbero una notevole diffusione le operazioni di *bugging*, i.e. l'inserimento di microfoni (cd. cimici) in luoghi sensibili quali proprietà private, ambasciate o camere d'albergo.[615] La giurisprudenza di riferimento, all'epoca, era racchiusa nel noto caso *Olmstead v. United States.* [616] Nel dispositivo della sentenza, una maggioranza di cinque giudici aveva sostenuto che fintantoché l'ingerenza non implica il *trespass* (intrusione fisica), non si può parlare di una vera e propria

---

[610] Costituzione degli Stati Uniti d'America, Emendamento IV.
[611] Si tratta di indagini concernenti: "*1)international terrorism* […] *2)espionage and other intelligence activities, sabotage, or assassination, conducted by, for, of on behalf of foreign powers, organizations, or persons* […] *3)foreign computer intrusions*"; U.S. Dep't of Justice, "The Attorney General's Guidelines for Domestic FBI Operations" [2008] 7; vd. U.S. Dep't of Justice "The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection" (U) [2003] 6-7; L R ATKINSON, "The Fourth Amendment's National Security Exceptions: Its History and Limits" [2013] 66 L Vand Rev 1357.
[612] S EDWARDS, *Barbary General: the Life of William H Eaton* (Prentice-Hall, 1968) 54-55; B F MELTON JR, *The First Impeachment* (Mercher University Press, 1988) 93; *cfr.* L R ATKINSON, *op. cit.* 1357.
[613] L R ATKINSON, *op. cit.* 1346-1347.
[614] Nel 1939 il Presidente Roosevelt aveva investito l'FBI di tutte le principali funzioni di *intelligence*: indagini in materia di spionaggio, controspionaggio e sabotaggio; vd, *Ibidem*.
[615] L R ATKINSON, *op. cit.* 1360.
[616] *Olmstead v. United States* [1928] 277 U.S. 438.

ricerca (*search*) ricompresa nella tutela del quarto emendamento.[617] Il giudice Brandeis, già citato nelle pagine precedenti per l'enorme contributo fornito col suo articolo "*The Right to Privacy*",[618] presentò una *dissenting opinion*. Il supremo *Justice* criticava duramente l'approccio dei suoi colleghi, anacronisticamente ancorato al diritto di proprietà dei beni materiali. La "santità" della sfera personale dell'individuo, sosteneva, può essere violata anche senza l'impiego della forza.[619]

Ciononostante, non solo il *bugging* è proseguito, ma negli anni è stato accompagnato da pratiche ben più intrusive.[620] Le perplessità sul piano costituzionale di operazioni condotte attraverso il *trespass* erano perfettamente note. In una corrispondenza tra lo storico direttore dell'FBI J. Edgar Hoover e lo *Assistant Attorney General* del tempo, T. Lamar Caudle, si legge: "*where there has been a physical trespass upon the premises occupied by the defendant* […] *the evidence obtained by that means would be inadmissible on the ground that it was obtained by an illegal search and seizure.*"[621] La risposta del *Bureau* fu di perseverare nell'impiego abituale di metodi d'indagine non approvati, evitando però di presentare in giudizio le prove raccolte in questo modo. Nonostante Caudle avesse esplicitamente definito tali metodi di ricerca "*illegal search*", Hoover diede vita ad una prassi ancora in auge ai giorni d'oggi: la cd. "*pure intelligence rule*".[622]

---

[617] P G MADRIÑAN, "Devil in the Details: Constitutional Problems Inherent in the Internet Surveillance Provisions of the USA PATRIOT Act of 2001" (2002-2003) 64 U Pitt L Rev 783-784; L R ATKINSON, *op. cit.* 1360; D GRAY & D CITRON: *op. cit.* 83-84; giurisprudenza in seguito confermata dal caso *Goldman v. United States* [1942] 316 U.S. 129, 134-135.

[618] *Cfr. supra*.

[619] *Olmstead v. United States* [1928] 277 U.S. 438: "*[The Framers] recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure, and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to let alone – the most comprehensive of rights, and the right most valued by civilized men.*"; D GRAY & D CITRON: *op. cit.* 85.

[620] E.g. intrusioni in case, uffici ed altri luoghi protetti al fine di raccogliere prove (cd. *black bag jobs*) o apertura di corrispondenza (*chamfering*): *cfr.* C0-1361.

[621] Federal Bureau of Investigation, U.S. Dep't of Justice, "Microphones: Policy Brief" [1966] 9; vd. anche A THEOHARIS, *From the Secret Files of J. Edgar Hoover*, Memorandum from Attorney General Howard McGrath for J. Edgar Hoover, Dir. (Ivan R. Dee, Inc. 1933) 137: "*[buggings that] involve trespass are in the area or the Fourth Amendment, and evidence so obtained and from leads so obtained is inadmissible* […] *[P]lease be advised I cannot authorize the installation of a microphone* involving a trespass *under existing law.*"; L R ATKINSON, *op. cit.* 1361, 1366.

[622] *Cfr.* D S KRIS & D WILSON, *National Security Investigations and Prosecutions* (Thomson/West Publ'g, 2007) §3.4: "*Because the Supreme Court has made clear that a warrantless government*

Applicando correttivi che la rendessero sufficientemente persuasiva per lo *Attorney General* in carica,[623] la regola consentì per decenni il ricorso a tecniche investigative senza mandato, i cui esiti non venivano mai sottoposti ad una corte giudicante. Il limite dell'inutilizzabilità probatoria, a conti fatti, permise al *Bureau* di sottrarsi alla censura giurisdizionale.

L'occasione per operare un *overruling* del caso *Olmstead* giunse solo nel 1967, con *Katz v. United States*.[624] Nel caso di specie, la Corte stabilì che l'intercettazione di conversazioni telefoniche, attraverso l'installazione di un apparecchio situato in un telefono pubblico, costituisce una ricerca (*search*). Ricade dunque nell'ambito applicativo del quarto emendamento, nonostante non ci sia intrusione fisica nella proprietà di alcuno.[625] Il pensiero del giudice Brandeis prevale dopo quasi quattro decadi: "*the Fourth Amendment protects people, not places*".[626]

Katz ha consentito ad un principio fondamentale in materia di *privacy* di fare breccia nel sistema statunitense: quello della ragionevole aspettativa (*reasonable expectation*). Per determinare se il contegno del Governo sia intrusivo (e quindi illegale in assenza di un mandato), il giudice deve appurare se nel contesto in cui è avvenuta l'intercettazione l'individuo avesse un'aspettativa di *privacy* che la società riconosce come ragionevole.[627] Ovviamente la presunzione di non essere sorvegliati è maggiore in casa propria ma, come insegna il caso *Katz*, non c'è una connessione necessaria fra *privacy* e proprietà privata.

---

trespass to install a microphone violated the Fourth Amendment, Attorney General Brownell's authorization […] *seemed to represent an assertion that «internal security» allowed government agents to engage in conduct that otherwise would violate the Fourth Amendment"*; per il testo del memorandum di Brownell cui si fa riferimento, vd. *Ibidem*: "*[t]he FBI has an intelligence function in connection with international security matters equally as important as the duty of developing evidence for presentation to the courts*"; vd. anche L R ATKINSON, *op. cit.* 1369: "*Director Hoover conceded that «[t]he information obtained from [trespassory] microphones* […] *is not admissible in evidence» but reasoned that if investigations remained «purely intelligence» operations – in other words, for nonevidentiary purposes – they would not run afoul of the constitutional difficulties the Bureau had previously encountered*".

[623] *Cfr.* Memorandum from Attorney General Herbert Brownell for J Edgar Hoover, Dir. [1954] FBI 1: "*in some instances the use of microphone surveillance is the only possible way of uncovering activities of espionage agents, possible saboteurs, and subversive persons* […] *[T]he Department should adopt that interpretation which will permit microphone coverage by the FBI in a manner most conductive to our national interest*".

[624] *Katz v. United States* [1967] 389 U.S. 347, 353; D GRAY & D CITRON: *op. cit.* 84.

[625] *Katz v. United States* [1967] 389 U.S. 353, 358-359; D GRAY & D CITRON: *op. cit.*; P G MADRIÑAN, *op. cit.*

[626] *Katz v. United States* [1967] 389 U.S. 351; D GRAY & D CITRON: *op. cit.*

[627] *Cfr. United States v. Jones* [2012] 132 S. Ct. 945, 950; D GRAY & D CITRON: *op. cit.* 85.

Nonostante la portata rivoluzionaria della sentenza, la prassi dei servizi segreti non mutò in maniera significativa. Al contrario si radicò più che negli anni precedenti il convincimento che, almeno per questioni di sicurezza nazionale, fosse possibile operare senza un'autorizzazione fornita *ex ante* dall'autorità giudiziaria.[628] Appartengono a questi anni le prime sentenze che, nel completo silenzio del legislatore, autorizzavano intercettazioni telefoniche senza mandato. L'unica condizione richiesta era che lo scopo dell'inquirente fosse quello di ottenere unicamente "*foreign intelligence information*".[629]

Il baluardo contro la formazione di un vero e proprio Stato di sorveglianza in America, paradossalmente, risiedeva nella stessa *pure intelligence rule*. Infatti, nessun giudice arrivò mai ad autorizzare l'assunzione di prove ottenute tramite mezzi di sorveglianza non autorizzati.[630] Tuttavia, non fu accordata la stessa protezione ai cittadini stranieri all'estero. In *Keith*, la Corte Suprema riconobbe la crescente diffusione dell'idea che "*warrantless surveillance, though impermissible in domestic security cases, may be constitutional where foreign powers are involved*".[631]

Riassumendo lo scenario fin qui descritto, si nota negli USA una forte discrasia tra dettato costituzionale e prassi dell'esecutivo, che arriva a snaturare il contenuto del quarto emendamento. Il giudice Brandeis (il quale non a caso può definirsi il padre della dottrina europea in materia di *privacy*) aveva intuito la portata della norma, concentrando la propria analisi sulla tutela offerta alla sfera

---

[628] Questa pratica *contra legem* trovava la sua giustificazione nell'interpretazione data dall'esecutivo ad una nota a piè di pagina presente in *Katz*: "Footnote 23: *Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case.*" Nonostante i termini siano piuttosto vaghi, il Governo fece affidamento su questa frase per riprendere la pratica di installare cimici ed altri dispositivi di sorveglianza senza mandato. Permanevano il limite delle esigenze di sicurezza nazionale e l'inutilizzabilità in giudizio delle prove così raccolte.

[629] *United States v. Clay* [1970] 430 F 2d 165, 170; *cfr*. *United States v. Hoffman*, 334 F Supp [1971] 504, 508.

[630] Durante l'amministrazione Nixon, il governo provò ad estendere la portata della *pure intelligence rule*, ma senza successo. Nelle memorie presentate in *United States v. United States District Court* [1972] 407 U.S. 297, si legge: "*in the course of such [warrantless national security] surveillance evidence may be obtained that indicates commission of a crime. In such an event the government contends that it would be fully warranted in using the evidence thus obtained in prosecuting the crime thus disclosed*"; vd. anche *Ivanov v. United States* [1969] 394 U.S. 165; L R ATKINSON, *op. cit.* 1382, 1388.

[631] *United States v. United States District Court* [1972] 407 U.S. 297; vd. anche casi analoghi e.g. *United States v. Smith* [1971] 321 F Supp 424, 425-426; *United States v. Buck* [1977] 548 F 2d 871, 875; *United States v. Butenko* [1974] 494 F 2d 593, 605; *United States v. Brown* [1973] 484 F 2d 418, 426; L R ATKINSON, *op. cit.*

privata della persona. L'esecutivo, di contro, ha da sempre sviato la discussione su una questione importante ma secondaria: l'utilizzabilità in giudizio di prove ottenute senza mandato. Eppure, c'è un problema diverso da considerare a monte di ciò. La *ratio* nel subordinare un'intercettazione alla previa autorizzazione del giudice è quella di valutarne la ragionevolezza, i.e. se la soppressione del diritto alla *privacy* per esigenze di polizia sia ragionevole nel caso di specie. L'istituto dell'inutilizzabilità è volto a sanzionare il ricorso ad un mezzo di ricerca della prova illegittimo, che perciò non doveva essere utilizzato in primo luogo. Il fatto che l'intrusione nella vita privata di una persona potesse essere arbitraria o *contra legem* non ha mai destato particolari preoccupazioni. Solo lo *Attorney General* Edward Levi, interpellato nel 1975 dalla cd. "*Church Committee*",[632] concesse che "*[i]t may be said that this [the pure intelligence rule] confuses rights and remedies; searches could be unreasonable even though no sanction followed*".[633] Ciononostante, anche Levi favorì un approccio pragmatico e difese la Regola in ragione dell'uso ormai protratto negli anni.

La dottrina recente, nel tentativo di trovare un fondamento giurisprudenziale più solido, ha proposto una soluzione ulteriore. Le indagini per la sicurezza nazionale, è stato sostenuto, per la loro stessa natura indicano l'esistenza di speciali esigenze di polizia. Per tale ragione, possono essere sussunte in una diversa eccezione già consolidata nella giurisprudenza di riferimento: la "*special needs doctrine*".[634] Questa si regge sull'assunto che "*a judicial warrant and probable cause are not needed where the search or seizure is justified by special needs, beyond the normal need for law enforcement*".[635] Dal momento che la sicurezza nazionale serve obiettivi militari, diplomatici o comunque politici,

[632] Si tratta della *United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, che chiamò Levi per discutere dei rapporti tra sorveglianza elettronica e quarto emendamento; vd. "The National Security Agency and Fourth Amendment Rights": Hearing on S. Res. 21 Before the Select Committee to Study Governmental Operations with Respect to Intelligence Activities [1979] 94 Cong 78, 101; *cfr.* L R ATKINSON, *op. cit.* 1385-1386.
[633] *Ibidem*.
[634] L R ATKINSON, *op. cit.* 1390.
[635] *Ashcroft v. al-Kidd* [2011] 131 S Ct 2074, 2081; la sentenza cita a sua volta *Vernonia Sch. Dist. 47J v. Acton* [1995] 515 U.S. 646, 653; L R ATKINSON, *op. cit.*

andrebbe sempre e comunque classificata come sottocategoria degli *special needs*.[636]

La Corte FISA [637] ha confermato questa posizione in due diverse sentenze.[638] Nonostante l'avallo ottenuto sul piano giurisprudenziale, però, ci sono forti perplessità sulla correttezza di una simile configurazione. Tra *special needs doctrine* e *pure intelligence rule*, in effetti, non ci sono differenze sostanziali. Entrambe forniscono all'esecutivo un'autorizzazione in bianco ad ingerirsi nella sfera privata del cittadino, evitando il vaglio di legittimità di una corte e qualsivoglia valutazione di necessità e proporzionalità. Senza un approccio caso per caso, che permetta di riconoscere l'adeguatezza dei mezzi di ricerca a seconda delle diverse situazioni, non è possibile garantire il sereno godimento del diritto alla *privacy*. Questo anche quando sul piatto della bilancia si trovano esigenze di sicurezza nazionale. Nella *concurrent opinion* del giudice Douglas in *Katz*, si legge infatti:

[*n*]*either the President nor the Attorney General is a magistrate. In matters where they believe national security may be involved they are not detached, disinterested, and neutral as a court or magistrate must be. Under the separation of powers created by the Constitution, Executive Branch is not supposed to be neutral and disinterested. Rather it should vigorously investigate and prevent breaches of national security and prosecute those who violate the pertinent federal laws. The President and Attorney General are properly interested parties, cast in the role of adversary, in national security cases […] I cannot agree that where spies and saboteurs are involved adequate protection of Fourth Amendment rights is assured when the President and Attorney General assume both the position of adversary-and-prosecutor and disinterested, neutral magistrate*.[639]

[636] L R ATKINSON, *op. cit.*
[637] Vd. paragrafo successivo.
[638] *In re* Sealed Case [2002] 310 F 3d 717, 745-746; *In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act [2008] 551 F 3d 1004, 1010-1011; *cfr.* L R ATKINSON, *op. cit.* 1391.
[639] *Katz v. United States* [1967] 389 U.S. 347, 357; P G MADRIÑAN, *op. cit.* 832.

2.4.2. La *privacy* negli USA dopo *Katz*: *Wiretap Statute,* FISA e USA PATRIOT Act

Alla fine degli anni '60 era ormai diffusa la consapevolezza che il governo ricorreva sistematicamente a intercettazioni telefoniche (*wiretaps*) illegali. Dopo che anche la Corte Suprema si fu espressa in *Katz*[640] il vuoto normativo esistente non poteva più essere ignorato dal Congresso.[641]

Nel 1968 venne perciò adottato il cd. *Wiretap Statute*,[642] una legge federale che per la prima volta regolava nelle indagini *interne* i poteri di controllo degli agenti governativi, bilanciandoli con il diritto alla *privacy* dei cittadini.[643] Riconoscendo la possibilità di abusi insita nelle tecniche di sorveglianza elettronica, il *Wiretap Statute* impone come requisito fondamentale l'autorizzazione del giudice. Per ottenerla il richiedente deve mostrare l'esistenza di una *probable cause*[644] e deve fornire altresì una descrizione specifica dei mezzi di comunicazione che saranno intercettati.[645] Sono previsti anche diversi altre garanzie, tra i quali merita di essere menzionata la possibilità per il giudice di richiedere una documentazione ulteriore rispetto a quella già fornita in un primo momento.[646] Inoltre, l'autorizzazione deve obbligatoriamente essere accordata per un periodo non superiore a quello strettamente necessario.[647]

Per ciò che concerne invece la sorveglianza *esterna*, in risposta ai lavori della *Church Committee*[648] il Parlamento redasse nel 1978 il *Foreign Intelligence Surveillance Act* (FISA).[649] Il corpo del testo, approvato oltre trenta anni fa, oggi

---

[640] Ma vedi anche *Berger v. New York* [1967] 388 U.S. 41.
[641] M F DOWLEY, "Government Surveillance Powers Under the USA PATRIOT Act: Is It Possible to Protect National Security and Privacy at the Same Time? A Constitutional Tug-of-War" (2002-2003) 36 Suffolk U L Rev 171.
[642] *Omnibus Crime Control and Safe Streets Act* 1968, Title III.
[643] M F DOWLEY, *op. cit.*; B D ROSEMAN, "Electronic Platform, E-mail and Privacy Issues" [2001] SG016 A L I – A B A 1165, 1166-1167; *cfr.* NINO M., *op. cit.* 734.
[644] Si tratta di un presupposto indicato dallo stesso quarto emendamento e ben noto nel diritto penale americano. Nell'ordinamento italiano è paragonabile ai "gravi indizi di reato" ex Art. 267 cpp.
[645] 18 U.S.C. §2518(3)(4); M F DOWLEY, *op. cit.* 172.
[646] 18 U.S.C. §2518(2).
[647] 18 U.S.C. §2518(5).
[648] Vd. *supra*.
[649] E B BAZAN, "The Foreign Intelligence Surveillance Act: an Overview of Selected Issues" [2008] Congressional Research Service 1.

costituisce soltanto il Titolo I di uno statuto che è stato soggetto a diversi rimaneggiamenti.[650]

Contrariamente a quanto avviene nelle indagini per la sicurezza interna, dottrina e giurisprudenza hanno sempre concordato nel non riconoscere la tutela del quarto emendamento ai non cittadini, soprattutto quando situati all'estero (i.e. *foreign intelligence*).[651] Con il FISA la disciplina dei mandati viene ricostruita,[652] subordinando anche in questo caso la sorveglianza elettronica ad un'autorizzazione giudiziale.[653] Allo stesso tempo viene istituita una corte federale specializzata: la Corte FISA (FISC), con giurisdizione esclusiva in materia.[654]

Il rilascio dei mandati è sottoposto a criteri decisamente più elastici, se comparati con il princpio della *probable cause*. Difatti, al giudice è sufficiente ritenere che esista il sospetto fondato (*significant purpose*) che l'obiettivo dell'intercettazione sia una potenza straniera od un suo agente.[655] Nonostante i difetti evidenziati, si può sostenere che lo statuto abbia apportato delle migliorie al quadro normativo lacunoso e caotico della *privacy* americana. La situazione, tuttavia, non era destinata a rimanere stabile.

Lo *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (USA PATRIOT *Act* o USAPA) del 2001 ha espanso notevolmente i poteri di controllo del Governo

---

[650] *Ibidem*, 2; L R ATKINSON, *op. cit.* 1396.
[651] Vd *supra*; per una diversa definizione di *foreign intelligence* vd. la descrizione contenuta nello stesso FISA, 50 U.S.C. §1801(e): "*«Foreign intelligence information» means—(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—*
(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
(A) the national defense or the security of the United States; or
(B) the conduct of the foreign affairs of the United States."
[652] L R ATKINSON, *op. cit.*
[653] 50 U.S.C. §1804; *Ibidem*.
[654] M F DOWLEY, *op. cit.* 173.
[655] 50 U.S.C. §1804(a)(6)(B); M F DOWLEY, *op. cit.*; NINO M., *op. cit.*

USA, sia in patria che all'estero.[656] Si tratta di uno statuto emergenziale, che in risposta agli attacchi terroristici dell'11 Settembre ha recato diverse modifiche al FISA.[657]

In primis lo USAPA ha modernizzato il Titolo III del FISA, in modo da garantire espressamente al governo l'intercettazione di mezzi di comunicazione informatici (e.g. e-mail e traffico dati).[658] Un secondo emendamento di rilievo riguarda il *roving wiretap*: all'FBI è consentito richiedere l'autorizzazione per talune intercettazioni senza specificare la linea telefonica, il computer od il diverso servizio da monitorare.[659] La disposizione più controversa è certamente contenuta nella sezione §215, la quale autorizza il *Bureau* a richiedere a determinati soggetti[660] la consegna di qualsiasi elemento concreto (*any tangible things*) relativo al terrorismo internazionale o ad attività di *intelligence* clandestine. Le perplessità maggiori derivano dal fatto che l'indagine non deve indicare un individuo specifico (è possibile l'accesso generico a qualunque *database*) e non è richiesta la presenza di una *probable cause* né di un mandato.[661]

2.4.3. Il FISA *Amendments Act* 2008 e la Corte FISA

Le maglie già deboli del FISA sono state ulteriormente sfaldate nel 2008, con l'approvazione del FISA *Amendments Act* (FAA).[662] Da quel momento infatti, è stata esplicitamente introdotta la possibilità di svolgere attività di sorveglianza senza mandato.[663] L'attuale sezione §702 FISA richiede solo due condizioni:

1) che l'obiettivo sia un non-cittadino, e che sia ragionevolmente ritenuto (*reasonably believed*) essere situato al di fuori degli Stati Uniti;

---

[656] M F DOWLEY, *op. cit.* 177.
[657] *Ibidem*; NINO M., *op. cit.*
[658] M F DOWLEY, *op. cit.* 178; USA PATRIOCT *Act*, §§209, 214, 216-217.
[659] M F DOWLEY, *op. cit.*; USA PATRIOCT *Act*, §206.
[660] Si tratta dei proprietari di hotel, motel, autonoleggi, biblioteche, librerie ed esercizi simili.
[661] USA PATRIOT Act §215; vd. le aspre critiche mosse dalla American Civili Liberties Union (ACLU): https://www.aclu.org/free-speech-national-security-technology-and-liberty/reform-patriot-act-section-215.
[662] Si segnala inoltre che il FAA era destinato a perdere efficacia una volta trascorsi cinque anni dall'approvazione, ma nel 2012 è stato riconfermato dal FISA *Amendments Act Reauthorization Act*: https://www.govtrack.us/congress/bills/112/hr5949/text.
[663] L R ATKINSON, *op. cit.* 1399.

2) che la raccolta di informazioni persegua solo scopi di *foreign intelligence*.[664]

La modifica produsse da subito serie preoccupazioni. Diveniva più concreta che mai la possibilità di dare il via ad una "*brave new era of US-based «*data mining*» operations by the NSA and [to] result in a substantial increase in warrantless «incidental acquisitions» of phone calls and email messages of American citizens and others in the United States*".[665] La rivelazione di PRISM e degli altri programmi di *mass surveillance* ha confermato queste preoccupazioni. Non solo: ha anche dimostrato che il monitoraggio sui cittadini americani è ben più stringente di una semplice "*incidental acquisition*".

La trattazione non sarebbe completa se non si accennasse anche al ruolo che la FISC ha avuto nella attuale crisi del diritto alla *privacy* in America. Per comprenderne i difetti strutturali, occorre considerare diversi elementi.

La Corte, si è detto, è stata istituita al fine di esercitare un controllo giurisdizionale sulle agenzie di *intelligence* americane e di garantire la legittimità delle intercettazioni autorizzate. Per ragioni di segretezza essa svolge solamente udienze a porte chiuse, alla presenza di un rappresentante del Governo. La capacità del Congresso di vigilare sull'operato della FISC, perciò, è limitata ad un rapporto annuale.[666] Redatto dallo *Attorney General*, esso indica solamente:

> *(a) the total number of applications made for orders and extensions of orders approving electronic surveillance under this subchapter; and*
>
> *(b) the total number of such orders and extensions either granted, modified, or denied.*[667]

Tutti questi elementi, unitamente all'elevatissimo tasso di approvazione delle *applications* presentate,[668] hanno giustificato un comprensibile scetticismo circa l'imparzialità della Corte.[669]

---

[664] 50 U.S.C. §1881(a).
[665] D G BARNUM, "Foreign Intelligence Surveillance in the United States: Update" (2008) 5 E H R L R 654.
[666] 50 U.S.C. §1806.
[667] *Ibidem*.
[668] R B WALTON, "Letter of the FISA Court President to the Chairman of the U.S. Senate Judiciary Committee Patrick J. Leahy about Certain Operations of the FISA Court", 29 July 2013. Nella lettera il Presidente Walton replica che "*[t]he annual statistics provided to Congress by the Attorney General [...] - frequently cited to in press reports as a suggestion that the Court's approval rate of application is over 99% - reflect only the number of* final *applications submitted*

Da un rapporto redatto dalla *Judiciary Committee* del Senato[670] si evince la posizione del Congresso, che riflette le opinioni appena esposte:[671]

> *[o]versight of the entire FISA process is hampered* […] *because the Congress and the public get no access to any work of the FISA Court, even work that is unclassified. This secrecy is unnecessary, and allows problems in applying the law to fester. There needs to be a healthy dialogue on unclassified FISA issues within Congress and the Executive branch and among informed professionals and interested groups. Even classified legal memoranda submitted by the DOJ[672] to, and classified opinions by, the FISA Court can reasonably be redacted to allow some scrutiny of the issues that are being considered. This highly important body of FISA law is being developed in secret, and, because they are ex parte proceedings, without the benefit of opposing sides fleshing out the arguments as in other judicial contexts, and without even the scrutiny of the public or the Congress.*[673]

Alle critiche mosse dalla Commissione, se ne possono aggiungere altre circa le modalità attraverso le quali sono nominati i giudici della Corte. Infatti, il FISA prevede che gli undici giudici del collegio siano designati *en bloc* dal Presidente della Corte Suprema degli Stati Uniti (*Chief Justice*).[674] Sebbene l'autorevolezza di questa figura e la pubblicità della nomina forniscano una garanzia di imparzialità, non si può ignorare che la procedura manchi di un autentico meccanismo di controllo. Nel sistema di "*check and balances*" americano, si tratta

---

to and acted on by the Court. These statistics do not reflect the fact that many applications are altered to prior or final submission or even withheld from final submission entirely, often after an indication that a judge would not approve them".

669 *Ibidem*.

670 P LEAHY, A SPECTER & C E GRASSLEY, "Interim Report on FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures" (February 2003): "*Working in a bipartisan manner in the 107th Congress, the Senate Judiciary Committee conducted the first comprehensive oversight of the FBI in nearly two decades. That oversight was aimed not at tearing down the FBI but at identifying any problem areas as a necessary first step to finding constructive solutions and marshaling the attention and resources to implement improvements. The overarching goal of this oversight was to restore confidence in the FBI and make the FBI as strong and as great as it must be to fulfill this agency's multiple and critical missions of protecting the United States against crime, international terrorism, and foreign clandestine intelligence activity, within constitutional and statutory boundaries.*"

671 Orientativamente, i maggiori attriti tra Congresso e FISC possono essere fatti risalire al periodo post-11 Settembre.

672 I.e. *Department of Justice*.

673 P LEAHY, A SPECTER & C E GRASSLEY, *op. cit.*

674 50 U.S.C. §1803.

di un'anomalia. Se si considera poi che lo stesso *Chief Justice* è nominato direttamente dal Presidente degli Stati Uniti, il rischio di una eccessiva politicizzazione del FISC diventa plausibile.[675]

Da ultimo, la vicenda *datagate* ha evidenziato come la Corte non rispetti pedissequamente i vincoli della propria giurisdizione. Si fa riferimento, in particolare, alla nota *application* con la quale la NSA richiedeva l'accesso ai metadati delle conversazioni telefoniche degli utenti del gestore "Verizon".[676] Nell'ordinanza della Corte si legge che "*[Verizon] shall produce to the National Security Agency (NSA) upon service of this Order, and continue production on an ongoing daily basis thereafter for the duration of this Order* […] *an electronic copy of the following tangible things:* all call data *detail records or "telephone metadata" created by Verizon communications (i) between the United States and abroad or (ii)* wholly within the United States, including local telephone calls".[677] (Enfasi aggiunta).

L'ultimo dato è sicuramente il più inquietante, giacché mostra come la FISC abbia deliberatamente approvato la sorveglianza non solo di "potenze straniere o agenti di potenze straniere",[678] ma anche dei cittadini americani. Ciò senza considerare che l'ordinanza, così formulata, viola palesemente gli obblighi internazionali assunti dagli USA ex Art. 17 ICCPR. Infatti, è difficile conciliare il controllo indiscriminato di "*all call detail records*"[679] con i principi di non arbitrarietà, necessità e proporzionalità che la Convenzione racchiude.

---

[675] Si segnala che il 19 Luglio 2013 è stato presentato un *bill* alla Camera dei Deputati per modificare il FISA ed investire direttamente il Presidente USA del potere di nominare i giudici della FISC. In ogni caso, la proposta di legge ha scarse probabilità di essere approvata: https://www.govtrack.us/congress/bills/113/hr2761#overview.

[676] United States Foreign Intelligence Surveillance Court, "In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From Verizon Business Network Services, Inc. on Behalf of MCI Communication Services, Inc. D/B/A Verizon Business Services" (4/25/2013).

[677] *Ibidem*.

[678] 50 U.S.C. §1804(a)(6)(B).

[679] L'importanza dei metadati è stata illustrata recentemente in ELECTRONIC FRONTIER FOUNDATION, "International Principles on the Application of Human Rights to Communications Surveillance" (July 10, 2013): https://en.necessaryandproportionate.org/text: "*[w]hen accessed and analyzed, communications metadata may create a profile of an individual's life, including medical conditions, political and religious viewpoints, associations, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications*".

3. Soluzioni Proposte

I paragrafi precedenti hanno mostrato l'evidente *gap* esistente tra gli standard americani ed europei nella tutela dei dati personali e del diritto alla *privacy*. Di seguito vengono presentate alcune tra le soluzioni più valide ricercate tanto a livello normativo che giurisprudenziale.

3.1. La negoziazione dello *Umbrella Agreement*

Nel rapporto del Comitato LIBE del Parlamento Europeo, il cd. *Umbrella Agreement* [680] viene indicato come la precondizione necessaria per sanare completamente il rapporto di fiducia tra USA e UE.[681] Dai lavori preparatori, che alla data attuale sono in stasi, si nota in effetti come i negoziati abbiano portato a dei risultati estremamente positivi. Lo scopo dell'Accordo, si legge, è quello di assicurare un alto livello di protezione delle informazioni personali e di potenziare la cooperazione tra Stati Uniti ed Unione Europea.[682] L'ambito applicativo, si noti, è limitato alla prevenzione, localizzazione e persecuzione dei reati, inclusi quelli legati al terrorismo.[683] L'intento è quello di riunire, in un'unica cornice, tanto i trasferimenti di dati tra autorità giudiziarie delle Parti, che tutti gli altri trasferimenti giustificati da accordi bilaterali (e.g. PNR e TFTP).[684] In questo modo sarà possibile armonizzare e rafforzare lo scenario attuale, fatto di accordi multilaterali, bilaterali e settoriali.

I principi su cui le parti hanno già trovato un accordo stabile sono i seguenti:

- Conservazione dei dati: i dati trasmessi non devono essere trattenuti per un periodo superiore a quello strettamente necessario e appropriato.[685] La durata del trasferimento deve essere resa pubblica. Nel caso di

[680] Il nome provvisorio è in realtà *Framework Agreement on Data Protection in the Field of Police and Judicial Cooperation.*
[681] European Parliament – Committee on Civil Liberties, Justice and Home Affairs, Report (2013/2188(INI)) §55.
[682] Council of the European Union, "EU-US data protection «Umbrella Agreement» - Commission Services Non-Paper on state of play of negotiations" (8761/14) Brussels, 9 April 2014.
[683] *Ibidem*, §2.2
[684] *Ibidem*; per approfondimenti sul PNR, vd. Cause Riunite C-317/04 e C-318/04; per il TFTP vd. *supra.*
[685] *Ibidem*, §3.1.; perché la durata si possa ritenere appropriata, entrano in gioco diversi fattori quali lo scopo del trattamento, la natura dei dati e l'impatto sui diritti della persona interessata (*cfr. Ibidem*).

trasferimenti di dati in massa (*bulk*), è imposta la predisposizione di una clausola specifica indicante un termine stabilito di comune accordo.[686]

- Trasferimenti successivi: per trasferimenti successivi a terzi, è necessario il previo consenso dello Stato che per primo ha inviato i dati. La decisione è subordinata alla valutazione di elementi quali lo scopo del trattamento ed il livello di protezione garantito. I trasferimenti in massa devono essere giustificati da esigenze specifiche. Devono inoltre essere approntati idonei meccanismi di comunicazione tra le autorità competenti.[687]
- Non discriminazione: le previsioni dello *Umbrella Agreement* si applicano egualmente ai cittadini di entrambe le Parti.[688]
- Processi automatizzati: le decisioni che affliggono i diritti dell'individuo non possono essere demandate ad un processo automatizzato di elaborazione dati (e.g. PNR e TFTP), eccetto che sia previsto espressamente da una legge nazionale e vengano fornite tutele appropriate.[689]
- Fughe di dati: nel caso di fughe accidentali di dati, devono essere adottate misure adeguate per mitigare il danno. L'evento deve essere notificato all'autorità che ha inviato i dati e, se opportuno, anche alla persona interessata. Eventuali eccezioni devono essere tassativamente previste.[690]
- Qualità ed integrità dei dati: i dati devono essere conservati con accuratezza, pertinenza, puntualità e completezza. Devono essere approntati procedimenti specifici per assicurarne la qualità e l'integrità.[691]
- Sicurezza: devono essere predisposti sistemi di sicurezza per prevenire le perdite accidentali, la distruzione illegittima dei dati o la loro pubblicazione non autorizzata. Solo al personale autorizzato deve essere consentito l'accesso.[692]

[686] *Ibidem*.
[687] *Ibidem*, §3.2.
[688] *Ibidem*, §3.3.
[689] *Ibidem*, §3.5.
[690] *Ibidem*, §3.6.
[691] *Ibidem*, §3.7.
[692] *Ibidem*, §3.8.

- Trasparenza: la persona interessata ha diritto (salve le dovute restrizioni) ad essere informato dello scopo del trattamento, dell'eventuale utilizzo futuro dei suoi dati, delle norme che giustificano tale trattamento, dell'identità dei terzi ai quali le informazioni relative possono essere comunicate, dei meccanismi di accesso, rettifica e di ricorso disponibili.[693]
- Documentazione: le Parti devono predisporre mezzi idonei a documentare la legittimità dei trattamenti, soprattutto al fine di consentire eventuali reclami.[694]

L'Accordo riconosce inoltre i principali diritti sostanziali introdotti dalla Direttiva 95/46/CE: accesso e rettifica. Qualora questi siano ingiustamente negati o uno qualunque dei principi sopra esposti sia violato, il soggetto interessato potrà attivare un ricorso amministrativo di fronte all'autorità competente (e.g. il Garante per la protezione dei dati personali).[695]

Oltre alla funzione giurisdizionale, le Autorità Garanti svolgono un ruolo essenziale di monitoraggio e supervisione. In particolare, è previsto che le Autorità di entrambe le parti svolgano consultazioni regolari per garantire l'effettiva applicazione dell'Accordo e la cooperazione tra le parti contraenti.[696]

Il potenziale dello *Umbrella Agreement* è significativo già allo stato attuale. Soprattutto, vengono coperti molti dei punti nevralgici dell'attuale questione *privacy*: trasparenza, accessibilità, supervisione da parte di un organo terzo e indipendente, possibilità di risarcimento. D'altro canto, molte questioni cruciali devono essere ancora affrontate: l'azionabilità di ricorsi giurisdizionali, la possibilità di limitare ulteriormente le finalità dei trattamenti e come disporre dei dati sensibili.[697] Inoltre, è auspicabile un maggior grado di approfondimento riguardo alla possibilità di accordare trasferimenti di dati in blocco.[698] Infatti, la profonda invasività della pratica la rende in via di principio incompatibile con la disciplina europea in materia di dati personali.

---

[693] *Ibidem*, §3.9.
[694] *Ibidem*, §3.10.
[695] *Ibidem*, §4.
[696] *Ibidem*, §4.5.
[697] *Ibidem*, §5.
[698] *Ibidem*, §3.1: "*transfer of «programme-based» (bulk) data*".

3.2. La ACLU: proposta di revisione per il *General Comment* 16

Nel Marzo 2014, la *American Civil Liberties Union* (ACLU) ha pubblicato sul proprio sito web un documento intitolato "*Privacy Rights in the Digital Age*".[699] Il nucleo centrale della trattazione è basilare: la chiave di volta per riformare la tutela della *privacy* in America è l'Art. 17 ICCPR. Come si è avuto modo di attestare *supra*, la Convenzione adotta una terminologia di ampio respiro, da cui deriva la necessità di ricorrere all'interpretazione fornita dalla HRC nel *General Comment* 16.[700] Questo, attestano gli autori della ACLU, arranca dietro lo sviluppo tecnologico degli ultimi decenni e, soprattutto, i nuovi mezzi di sorveglianza impiegati dalle agenzie di *intelligence*.

La versione "attualizzata" del GC16 riscrive le seguenti voci:

- Il termine "casa": quando lo ICCPR fu redatto, Internet era ancora giovane. L'abitazione di un individuo oggi comprende anche spazi digitali come siti web e caselle di posta elettronica.[701]
- La "corrispondenza": include tutte le forme di comunicazione. I metadati, giacché rivelano diverse informazioni relative alla corrispondenza, meritano lo stesso grado di tutela.[702]
- "Interferenze illegittime":[703] viene proposto un test per verificare la legittimità di ogni eventuale intrusione nella vita privata della persona.[704] "*First, the interference must be consistent with the provisions, aims, and objectives of the Covenant. Second, the interference must be pursuant to, and in accordance with, enacted law (including international law). Third, the domestic statutory framework must be accessible and ensure that any interference with privacy interests is reasonably foreseeable to the person*

[699] ACLU, "Privacy Rights in the Digital Age" [2014] ACLU Foundation: https://www.aclu.org/privacyrights.
[700] Vd. *supra*.
[701] ACLU, *op. cit.* §C(3)(a).
[702] *Ibidem*, §C(3)(b).
[703] *Cfr. Ibidem*, Appendix I §18: "*The term «interference» includes, among other things, the simple collection or storage of personal information or data, as well as any manual or automated searching, review, obstruction, or diversion of communications*".
[704] *Ibidem*, §D(2).

concerned. Fourth, domestic law must be «precise» and «clearly» defined."[705]

- Non arbitrarietà:[706] per non essere arbitraria, l'intrusione dello Stato deve perseguire uno scopo legittimo, avere una connessione razionale con tale scopo e mantenere un equo bilanciamento tra l'obiettivo perseguito ed i diritti della persona interessata.[707] La sorveglianza indiscriminata *en masse* è di per sé contraria all'Art. 17 ICCPR. Anche le forme di sorveglianza legittime devono comunque essere sottoposte al controllo giurisdizionale. Le vittime di abusi devono avere accesso effettivo ad una forma di riparazione congrua.[708]
- Controllo giurisdizionale ed amministrativo: viene riconfermata la necessità di un effettivo controllo delle autorità di sorveglianza. Il tribunale competente a giudicare in materia deve essere pubblico, terzo, imparziale ed istituito per legge. Anche l'autorità amministrativa preposta deve fornire adeguate garanzie di imparzialità e trasparenza.[709]
- Applicazione extraterritoriale del diritto alla *privacy*: l'Art. 17 ICCPR deve applicarsi ovunque si estenda la giurisdizione dello Stato. Nel concetto di giurisdizione va ricompreso anche il potere di controllo virtuale. La tutela accordata agli stranieri deve essere coerente col principio di non discriminazione.[710]

3.3. La teoria della *quantitative privacy*

Nei paragrafi precedenti sono state riportate delle proposte di indubbio interesse, capaci di avere un impatto decisivo sulla problematica in esame.

[705] *Ibidem*, Appendix I §21.
[706] *Cfr. Ibidem*, Appendix I §27: *"A non-arbitrary, privacy-infringing measure must satisfy the following criteria. First, the interference must have a legitimate purpose, understood in the context of the Covenant. Second, the interference must be suitable; namely it must be capable of achieving its stipulated aim. More specifically, there must be a rational connection between the interference and the aim. Third, the interference must be strictly necessary, and should be the least intrusive means of realizing its aim. Fourth, the interference must be fairly balanced in relation to the purpose sought to be achieved.*"
[707] *Ibidem*, §D(3).
[708] *Ibidem*, §D(3)(b).
[709] *Ibidem*, §D(3)(e).
[710] *Ibidem*, §D(3)(f); per il principio di non discriminazione vd. anche Art. 2(1) ICCPR e *General Comment* 34 della HRC.

Ciononostante, è innegabile che nessuna delle due potrà realisticamente portare a dei risultati concreti nel breve periodo. In un sistema di Common Law come quello statunitense, per assistere ad una riforma normativa in tempi brevi bisogna piuttosto fare affidamento sulla *case law*, la giurisprudenza delle Corti superiori.

Prima ancora che il *Guardian* pubblicasse i primi articoli su Edward Snowden o che anche solo le parole NSA e *whistleblower* divenissero di dominio pubblico, la Corte Suprema degli Stati Uniti si pronunciava in *United States v. Jones*.[711] Nel caso in questione emerse che l'imputato era stato tracciato dagli inquirenti per quattro settimane, mediante un localizzatore GPS.[712] Nelle *concurring opinions*, diversi giudici espressero forti dubbi di incostituzionalità circa le crescenti capacità di controllo delle autorità di polizia.[713]

Come asserito dal giudice Ginsburg: "*the whole of one's movements over the course of a month is not* actually *exposed to the public because the likelihood anyone will observe those movements is effectively nil*".[714] Basandosi sul principio della *reasonable expectation,*[715] Ginsburg intuiva come le moderne tecniche di intercettazione siano capaci di erodere la *privacy* del cittadino ben oltre le sue aspettative. Si può allora affermare che tutti godono della *reasonable expectation* di non essere costantemente sorvegliati dal Governo.[716]

Tale approccio al diritto alla *privacy* è stato definito "quantitativo" (cd. *quantitative privacy*). Se estrapolato dal caso di specie, può tradursi come segue:[717] ogniqualvolta sia attuata una sorveglianza ampia ed indiscriminata, al cittadino è garantita la protezione del quarto emendamento.[718] Ciò significa che senza lo specifico mandato di un giudice, l'ingerenza del Governo nella vita privata dell'individuo è illegittima.[719]

---

[711] *United States v. Jones* [2012] 132 S Ct 945, 954; D GRAY & D CITRON, *op. cit.* 67.
[712] D GRAY & D CITRON, *op. cit.* 67-68.
[713] *United States v. Jones* [2012] 132 S Ct, vd. le *concurring opinions* dei giudici Alito e Sotomayor.
[714] *United States v. Jones* [2012] 132 S Ct 558, 563; D GRAY & D CITRON, *op. cit.* 88.
[715] Vd. *supra* il caso *Katz.*
[716] D GRAY & D CITRON, *op. cit.*
[717] *Ibidem*, 88-89.
[718] *Ibidem*, 101.
[719] *Ibidem*, 102: "*If a court finds that a challenged technology is capable of broad and indiscriminate surveillance by its nature, or is sufficiently inexpensive and scalable so as to present no practical barrier against its broad and indiscriminate use, then granting law enforcement unfettered access to that technology would violate reasonable expectations of quantitative privacy*"; vd. anche *Kyllo v. United States* [2001] 533 U.S. 34: "*[the Court must not]*

La giurisprudenza esistente, come dimostrato, possiede già tutti gli elementi per dichiarare l'illegittimità dei programmi della NSA, anche quando autorizzati dalla FISC. Tuttavia, bisogna sottolineare che la portata di *Jones* è limitata. Se da una parte statuisce che la *bulk data collection* dei cittadini americani è contraria ai principi del quarto emendamento,[720] poco o nulla è detto con riferimento al trattamento dei cittadini stranieri all'estero (i.a. i cittadini UE). È a questo punto che entrano in gioco gli strumenti normativi internazionali. Ciò che si augura è la ripresa dei lavori sullo *Umbrella Agreement* ed una più matura consapevolezza, da parte del Governo Americano, degli obblighi scaturenti ex Art. 17 ICCPR. Il principio di non discriminazione, infatti, ne impone l'eguale applicazione tanto nei confronti dei propri cittadini, che di quelli stranieri.

Pertanto, le tre "soluzioni" illustrate nelle pagine precedenti non devono considerarsi tra loro alternative. Sono parti di uno stesso schema che, operando su fronti diversi, può contribuire al risanamento della sfiducia globale nei servizi segreti americani e all'evoluzione della disarticolata tutela della *privacy* negli Stati Uniti.

permit police technology to erode the privacy guaranteed by the Fourth Amendment"; D GRAY & D CITRON, *op. cit.* 105.

[720] D GRAY & D CITRON, *op. cit.* 102: "*we see no reason why any citizen could not bring a Fourth Amendment claim challenging law enforcement's unfettered access to a surveillance technology or the Fourth Amendment sufficiency of a legislative or executive regulatory scheme governing law enforcement's access to a surveillance technology. After all, each of us has an equal share in the right of the people to be secure from the vagaries of a surveillance state*".

CAPITOLO III: ATTIVITÀ DI *INTELLIGENCE* IN TEMPO DI GUERRA

1. *Intelligence* tra parti belligeranti

Tradizionalmente, nel diritto internazionale pubblico, si può tracciare una linea di demarcazione tra regole applicabili in tempo di pace ed in tempo di guerra. Si tratta di realtà nettamente distinte, che in larga misura si escludono a vicenda: "una volta che sia stato fatto ricorso alla forza armata, i rapporti tra gli Stati in conflitto non sono più disciplinati dal diritto di pace ma dal diritto di guerra".[721] Con quest'ultima locuzione si richiama comunemente il solo *jus in bello*, vale a dire quel nutrito *corpus* di prescrizioni volte a regolare la violenza bellica. Vi rientrano anche i rapporti tra belligeranti e neutrali,[722] nonché la protezione dei civili e delle vittime del conflitto.[723] Con l'apertura alla ratificazione dei primi due Protocolli Addizionali alle Convenzioni di Ginevra del 1949, si può dire che la disciplina sia stata sostanzialmente unificata nel Diritto Internazionale Umanitario (DIU).[724]

Resta invece escluso lo *jus ad bellum*, che è lo strumento impiegato per determinare in quali casi si sia fatto illegittimamente ricorso alla forza armata.[725]

Anche in materia di *intelligence* lo schema normativo cambia sensibilmente in tempo di guerra (*rectius* nel corso di un "conflitto armato").[726] La maggior parte delle disposizioni esistenti, però, si concentra sullo spionaggio. Come è stato ribadito in più occasioni, questa particolare forma di HUMINT è solo la sottocategoria di un fenomeno ben più ampio. Regole indirizzate all'*intelligence gathering* in senso lato sono rare, probabilmente perché la collezione di dati riguardanti il nemico è un mero fatto. Durante il conflitto, le parti belligeranti sono perfettamente consapevoli ed accettano che l'avversario raccolga

[721] RONZITTI N., *Introduzione al Diritto Internazionale* (Giappichelli, 4a edn, 2013) 451.
[722] I.e. Il cd. "diritto dell'Aja"; *cfr. Ibidem*, 452.
[723] Cd. "diritto di Ginevra"; *Ibidem*.
[724] *Ibidem*.
[725] *Ibidem*, 451.
[726] Dopo la costituzione della Società delle Nazioni e soprattutto dell'ONU, le dichiarazioni di guerra sono cadute in disuso. Ciò non ha impedito la prosecuzione di operazioni militari, giustificate ad altro titolo. Vd. Carta delle Nazioni Unite, Artt. 2(4), 51; *cfr*. RONZITTI N., *op. cit.* 452.

informazioni e.g. sulla posizione di basi militari, fabbriche d'armi, stazioni radiofoniche, ponti ed altri *target* di varia natura.[727]

Cionondimeno, qualche raro riferimento normativo esiste. Ispirandosi alla Dichiarazione di Bruxelles (1874),[728] la Convenzione dell'Aja del 1899 attesta:

> *Les ruses de guerre et l'emploi des moyens nécessaires pour se procurer des renseignements sur l'ennemi et sur le terrain sont considérés comme «licites».*[729]

L'articolo fu riportato *verbatim* nella Convenzione dell'Aja del 1907, che sostituisce la precedente nei rapporti tra le parti contraenti.[730]

Con "stratagemmi di guerra" (*ruses de guerre*) la norma in questione fa riferimento a tutte quelle azioni che hanno lo scopo di ingannare l'avversario. [731] Pacificamente, le *ruses de guerre* sono tollerate nel diritto umanitario, purché non sfocino in atti di perfidia.[732] Aver collocato nel medesimo articolo anche il

---

[727] *Cfr*. ICRC, "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977: Commentary – Spies", 562.

[728] Projet d'une Déclaration internationale concernant les lois et coutumes de la guerre. Bruxelles, 27 août 1874, Art. 14: "*Les ruses de guerre et l'emploi des moyens nécessaires pour se procurer des renseignements sur l'ennemi et sur le terrain (sauf les dispositions de l'art. 36) sont considérés comme «licites»*"; il rinvio all'Art. 36 riguarda la popolazione civile nei casi di occupazione: "*La population d'un territoire occupé ne peut être forcée de prendre part aux opérations militaires contre son propre pays*". Evidentemente, la raccolta di informazioni è assimilata alle "*opérations militaires*".

[729] *Convention (II) concernant les lois et coutumes de la guerre sur terre* (La Haye, 29 juillet 1899), Art. 24.

[730] *Convention (IV) concernant les lois et coutumes de la guerre sur terre* (La Haye, 18 octobre 1907), Art. 4.

[731] J M HENCKAERTS & L DOSWALD-BECK, *Customary International Humanitarian Law Volume I: Rules* (Cambridge, 2009) 204; per alcuni esempi di *ruses de guerre* vd. *Ibidem*: "*surprises; ambushes; feigning attacks, retreats or flights; simulating quiet and inactivity; giving large strongpoints to a small force; constructing works, bridges, etc. which are not intended to be used; transmitting bogus signal messages, and sending bogus despatches and newspapers with a view to their being intercepted by the enemy; making use of the enemy's signals, watchwords, wireless code signs and tuning calls, and words of command; conducting a false military exercise on the wireless on a frequency easily interrupted while substantial troop movements are taking place on the ground; pretending to communicate with troops or reinforcements which do not exist; moving landmarks; constructing dummy airfields and aircraft; putting up dummy guns or dummy tanks; laying dummy mines; removing badges from uniforms; clothing the men of a single unit in the uniforms of several different units so that prisoners and dead may give the idea of a large force; and giving false ground signals to enable airborne personnel or supplies to be dropped in a hostile area, or to induce aircraft to land in a hostile area.*"

[732] Vd. *Convention de la Haye* 1907, Art. 23(b)(f); *I Protocole Additionnel aux Conventions de Genève du 1949*, Art. 37(1): "*Il est interdit de tuer, blesser ou capturer un adversaire en recourant à la perfidie. Constituent une perfidie les actes faisant appel, avec l'intention de la tromper, à la bonne foi d'un adversaire pour lui faire croire qu'il a le droit de recevoir ou l'obligation d'accorder la protection prévue par les règles du droit international applicable dans les conflits*

riferimento ai "mezzi occorrenti per procacciarsi delle informazioni", ha un significato particolare. Considerando le limitate disponibilità tecnologiche esistenti oltre un secolo fa, è probabile che anche tale norma fosse prevalentemente indirizzata a forme di *intelligence* condotte da agenti operativi i.e. allo spionaggio. Questo, essendo caratterizzato da segretezza ed inganno, veniva giocoforza assimilato alle *ruses*.

Ovviamente l'Art. 24 può essere esteso anche alle più moderne tecniche impiegate per la raccolta di informazioni (e.g. droni, satelliti e *hacking* di sistemi informatici), ma così facendo ci si discosta dall'originale *ratio* della norma. Come si vedrà *infra*, non è tanto l'acquisizione di informazioni segrete a richiedere una regolamentazione specifica. L'aspetto più delicato è *come* tali dati siano carpiti, i.e. quale sia il regime giuridico da applicare al combattente penetrato clandestinamente tra le linee nemiche.

Forse l'unica eccezione a quanto appena detto è contenuta nell'Art. 28(2) del I Protocollo Addizionale del 1977:

> *Les aéronefs sanitaires ne doivent pas être utilisés pour rechercher ou transmettre des renseignements de caractère militaire et ne doivent pas transporter de matériel destiné à ces fins* […]

Impiegando un aeromobile ovviamente non si compiono atti di spionaggio, bensì di SIGINT (e.g. intercettazione di segnali radio) o al massimo IMINT (e.g. voli di ricognizione). È vero, come affermato nelle pagine precedenti,[733] che la sorveglianza aerea ha molto in comune con lo spionaggio, ma la *ratio* del presente articolo è un'altra e va ricercata nella posizione privilegiata che il DIU garantisce ai mezzi di soccorso.[734] Si tratta di un divieto generale, che coinvolge qualsiasi

---

armés"; l'Art. 37(2) detta la disciplina attuale in materia di *ruses de guerre*: "*Les ruses de guerre ne sont pas interdites. Constituent des ruses de guerre les actes qui ont pour but d'induire un adversaire en erreur ou de lui faire commettre des imprudences, mais qui n'enfreignent aucune règle du droit international applicable dans les conflits armés et qui, ne faisant pas appel à la bonne foi de l'adversaire en ce qui concerne la protection prévue par ce droit, ne sont pas perfides. Les actes suivants sont des exemples de ruses de guerre : l'usage de camouflages, de leurres, d'opérations simulées et de faux renseignements.*"

[733] Vd. Capitolo I, §2.8.2.

[734] J M HENCKAERTS & L DOSWALD-BECK, *Customary International Humanitarian Law Volume I: Rules* (Cambridge, 2009), 98: "*Rule 29. Medical transports assigned exclusively to medical transportation must be respected and protected in all circumstances. They lose their protection if they are being used, outside their humanitarian function, to commit acts harmful to the enemy.*"

persona od oggetto che goda di questa protezione speciale:[735] i trasporti medici devono essere impiegati unicamente per il fine loro proprio.

In sintesi, il diritto umanitario si cura di dettare regole (quasi) esclusivamente con riferimento alle spie: cosa sia loro consentito durante le ostilità e quali diritti siano loro attribuiti.[736] Gli aspetti che concernono l'entità delle informazioni trasmesse, la loro reale utilità strategica o il danno provocato dall'atto di spionaggio, sono lasciati in secondo piano.

2. Spionaggio in tempo di guerra

Anche nei conflitti più recenti, lo spionaggio rimane una risorsa imprescindibile per i belligeranti. Infatti, per quanto avanzati possano essere gli strumenti di SIGINT, alcuni segreti della fazione avversaria sono accessibili solo con il contributo di un agente sul campo.[737]

2.1. Le prime codificazioni

Per descrivere i caratteri distintivi della spia, la prima risorsa alla quale attingere è il *Lieber Code*. Pur non trattandosi di una convenzione internazionale, tale opera costituisce il tentativo più risalente di dare forma al diritto della guerra. Prima di allora, il principale riferimento per i belligeranti era la consuetudine.[738] L'Art. 88 stabilisce che:

> *A spy is a person who secretly, in disguise or under false pretense, seeks information with the intention of communicating it to the enemy.*
>
> *The spy is punishable with death by hanging by the neck, whether or not he succeed in obtaining the information or in conveying it to the enemy.*

[735] ICRC, "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977: Commentary – Restrictions on Operations of medical Aircraft", 300 §1052.
[736] ICRC, "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977: Commentary – Spies", 562 §1756.
[737] *Ibidem*; Y DINSTEIN, *The Conduct of Hostilities Under the Law of Armed Conflict* (Cambridge University Press, 2004) 241 §598.
[738] Le "Instructions for the Government of Armies of the United States in the Field (*Lieber Code*), 24 April 1863" sono il frutto del lavoro di Francis Lieber, professore alla Columbia University durante la guerra di secessione americana. Sebbene fossero vincolanti solo tra le forze statunitensi, hanno fornito un contributo essenziale alla Dichiarazione di Bruxelles del 1874 e alle successive Convenzioni dell'Aia.

Il primo periodo non presenta differenze sostanziali rispetto alla definizione di spia presentata nel Capitolo I.[739] Tuttavia, il ricorso all'inganno ("*in disguise or under false pretense*") qui è considerato particolarmente grave, tanto da comportare la pena capitale.[740] La stessa pena è riservata ad esploratori e soldati sorpresi presso le linee nemiche con indosso le insegne della fazione avversaria.[741]

Il secondo periodo dell'Art. 88 conferma quanto sostenuto pocanzi: non è rilevante che le informazioni siano utili o meno alla parte belligerante. In entrambi i casi è prevista l'impiccagione.

Le regole ivi descritte si applicano immutate anche a chi, per ottenere informazioni dal nemico, faccia un uso improprio della bandiera bianca:

> *If it be discovered, and fairly proved, that a flag of truce has been abused for surreptitiously obtaining military knowledge, the bearer of the flag thus abusing his sacred character is deemed a spy.*[742]

In generale, sono puniti duramente tutti i comportamenti volti a ferire il nemico in modo occulto o sleale, sebbene l'inganno in sé sia ammesso come "*just and necessary means of hostility*".[743]

Il Codice ha anche il merito di aver introdotto una regola che, con le opportune modifiche, è ancora valida: se catturata dopo essersi ricongiunta con il proprio esercito, la spia non sarà più soggetta alle pene appena descritte. Sarà semplicemente tenuta sotto stretta osservazione in forza della sua pericolosità.[744]

A distanza di undici anni dalla pubblicazione del *Lieber Code*, la Dichiarazione di Bruxelles offre un nuovo contributo alla disciplina. L'Art. 19, aprendo la sezione "*des espions*", attesta che:

---

[739] Vd. *supra*: Capitolo I, §1.3.
[740] *Cfr.* G B DEMAREST, *op. cit.* 333.
[741] *Lieber Code*, Art. 83: "*Scouts, or single soldiers, if disguised in the dress of the country or in the uniform of the army hostile to their own, employed in obtaining information, if found within or lurking about the lines of the captor, are treated as spies, and suffer death.*"
[742] *Ibidem*, Art. 114.
[743] *Ibidem*, Art. 101: "*While deception in war is admitted as a just and necessary means of hostility, and is consistent with honorable warfare, the common law of war allows even capital punishment for clandestine or treacherous attempts to injure an enemy, because they are so dangerous, and it is difficult to guard against them.*"
[744] *Ibidem*, Art. 104: "*A successful spy or war-traitor, safely returned to his own army, and afterwards captured as an enemy, is not subject to punishment for his acts as a spy or war-traitor, but he may be held in closer custody as a person individually dangerous.*"

[n]e peut être considéré comme espion que l'individu qui, agissant clandestinement ou sous de faux prétextes, recueille ou cherche à recueillir des informations dans les localités occupées par l'ennemi, avec l'intention de les communiquer à la partie adverse.

La definizione indica tassativamente le condizioni necessarie per riconoscere la spia nemica: clandestinità, inganno e l'intenzione di raccogliere informazioni utili all'avversario. Di nuovo, non è rilevante che l'operazione sia portata a termine.

Ex Art. 20, la spia colta sul fatto sarà giudicata secondo le leggi nazionali dell'esercito che ha eseguito la cattura.[745] Se ne ricava che la sanzione prevista non è più *sic et simpliciter* la pena capitale, ma sarà necessario un processo. Altresì, ciò comporta implicitamente che alla spia non venga riconosciuto lo status di prigioniero di guerra come a qualunque altro legittimo combattente. La conferma è contenuta all'Art. 21, che descrive la situazione opposta:

L'espion qui rejoint l'armée à laquelle il appartient et qui est capturé plus tard par l'ennemi est traité comme prisonnier de guerre et n'encourt aucune responsabilité pour ses actes antérieurs.

La spia ricongiuntasi con la propria fazione, se successivamente catturata, riceve il trattamento dei prigionieri di guerra. Di contro, se viene colta sul fatto sarà sottoposta alla giurisdizione penale ordinaria.

Si tratta di una norma per certi versi paradossale, che va intesa come un deterrente più che una punizione.[746] Quando la spia ha ormai compiuto la propria missione, viene meno l'interesse a sanzionare azioni che, per il diritto dei conflitti armati, non sono criminose.[747]

La Dichiarazione contiene un'ultima disposizione in materia, l'Art. 22, nel quale sono sintetizzate molte delle tematiche già anticipate.[748] Innanzitutto, è

---

[745] Dichiarazione di Bruxelles, Art. 20: "*L'espion pris sur le fait sera jugé et traité d'après les lois en vigueur dans l'armée qui l'a saisi.*"
[746] G B DEMAREST, *op. cit.* 332.
[747] *Ibidem.*
[748] "*Les militaires non déguisés qui ont pénétré dans la zone d'opérations de l'armée ennemie, à l'effet de recueillir des informations, ne sont pas considérés comme espions.*
De même, ne doivent pas être considérés comme espions, s'ils sont capturés par l'ennemi: les militaires (et aussi les non-militaires accomplissant ouvertement leur mission) chargés de transmettre des dépêches destinées soit à leur propre armée, soit à l'armée ennemie.
A cette catégorie appartiennent également, s'ils sont capturés, les individus envoyés en ballon pour transmettre les dépêches, et, en général, pour entretenir les communications entre les diverses parties d'une armée ou d'un territoire."

definitivamente chiarito che la discriminazione fra legittimo combattente e spia deriva da una sola circostanza: quest'ultima non indossa l'uniforme del proprio esercito. Non potrebbe essere altrimenti, vista la natura delle sue mansioni. Di contro, il militare intenzionato a raccogliere informazioni, sorpreso oltre le linee nemiche, non riceve sanzioni particolari purché indossi regolarmente l'uniforme. Sarà trattato come un prigioniero di guerra. Lo stesso vale per coloro che (militari o meno) si siano introdotti nella zona operativa del nemico per trasmettere o ricevere corrispondenza.

Si noti che il testo della Dichiarazione di Bruxelles non fu mai ratificato, a causa dell'opposizione di alcuni governi.[749] Tuttavia, insieme al manuale di Oxford del 1880,[750] costituisce una solida base per il Regolamento allegato alla Convenzione dell'Aia del 1907.[751] Questo detta la disciplina ancora vigente per ciò che concerne la guerra via terra,[752] ed in merito allo spionaggio prevede che:

> *[n]e peut être considéré comme espion que l'individu qui, agissant clandestinement ou sous de faux prétextes, recueille ou cherche à recueillir des informations dans la zone d'opérations d'un belligérant, avec l'intention de les communiquer à la Partie adverse.*
>
> *Ainsi les militaires non déguisés qui ont pénétré dans la zone d'opérations de l'armée ennemie, à l'effet de recueillir des informations, ne sont pas considérés comme espions. De même, ne sont pas considérés comme espions: les militaires et les non militaires, accomplissant ouvertement leur mission, chargés de transmettre des dépêches destinées, soit à leur propre armée, soit à l'armée ennemie* […][753]

---

[749] ICRC, Risorse Online: http://www.icrc.org/applic/ihl/dih.nsf/TRA/135?OpenDocument&.

[750] *The Laws of War on Land* (Oxford 9 Settembre 1880), Art.24: "*Individuals may not be regarded as spies, who, belonging to the armed force of either belligerent, have penetrated, without disguise, into the zone of operations of the enemy, nor bearers of official dispatches, carrying out their mission openly, nor aeronauts*".

[751] ICRC, Risorse Online: http://www.icrc.org/applic/ihl/dih.nsf/INTRO/195.

[752] La Convenzione dell'Aia del 1899 presenta le stesse disposizioni, ma rimane valida solo tra gli Stati parti che non abbiano ratificato anche la Convenzione del 1907. Il primo Protocollo Addizionale alle Convenzioni di Ginevra del 1949 ha parzialmente riconfermato e sviluppato le regole ivi contenute. *Cfr*, ICRC, Risorse Online: http://www.icrc.org/dih/INTRO/150?OpenDocument; vd G B DEMAREST, *op. cit.* 334.

[753] *Règlement concernant les lois et coutumes de la guerre sur terre* (La Haye, 18 octobre 1907), Art. 29.

Come si percepisce ad una prima lettura, molto del dettato normativo di Bruxelles è stato ripreso fedelmente. Innanzitutto non mutano penalità e garanzie per la spia catturata: "*l'espion pris sur le fait ne pourra être puni sans jugement préalable*".[754] Una volta catturato, l'agente segreto deve essere regolarmente processato. Sarà sottoposto alla giurisdizione nazionale dello Stato che ha eseguito la cattura.

Rimane comunque valida la deroga accordata alle spie catturate dopo essersi ricongiunte al proprio esercito: *"[l]'espion qui, ayant rejoint l'armée à laquelle il appartient, est capturé plus tard par l'ennemi, est traité comme prisonnier de guerre et n'encourt aucune responsabilité pour ses actes d'espionnage antérieurs."*[755]

Tra Dicembre 1922 e Febbraio 1923, una Commissione di giuristi presieduta da John Bassett Moore tenne una serie di incontri all'Aia.[756] Il frutto dei lavori del gruppo fu un *corpus* di regole sulla guerra via aria, che non manca di affrontare la questione dello spionaggio:

> *Un individu, se trouvant à bord d'un aéronef belligérant ou neutre, ne peut être considéré comme espion que si, agissant clandestinement ou sous de faux prétextes, il recueille ou cherche à recueillir, en cours de vol, des informations dans la juridiction belligérante ou dans la zone d'opérations d'un belligérant, avec l'intention de les communiquer à la partie adverse.*[757]

Anche le presenti Regole sulla Guerra Aerea si concentrano su atti di spionaggio *stricto sensu*, mancando di imporre limiti o restrizioni e.g. all'osservazione aerea.[758] Questo perché, è bene ribadirlo, l'*intelligence gathering* non è un fenomeno regolato dal diritto dei conflitti armati. Ne risulta una disciplina parallela a quella dettata per i conflitti via terra, cui tra l'altro è fatto espresso rinvio.[759]

---

[754] *Ibidem*, Art. 30.
[755] *Ibidem*, Art. 31.
[756] ICRC, Risorse Online: http://www.icrc.org/ihl/INTRO/275?OpenDocument.
[757] *Règles de la guerre aérienne élaborées par une commission de juristes à La Haye* (décembre 1922 – février 1923), Art. 27.
[758] G B DEMAREST, *op. cit.* 335.
[759] *Règles de la guerre aérienne*, Art. 28: "*Les faits d'espionnage commis, après avoir quitté l'aéronef, par des membres de l'équipage d'un aéronef ou des passagers transportés par lui, restent soumis aux dispositions du Règlement concernant les lois et coutumes de la guerre sur*

Analogamente alla Dichiarazione di Bruxelles, le *Règles* del 1922 non furono mai tradotte in uno strumento convenzionale e sono pertanto prive di efficacia vincolante. La loro utilità sta nell'aver fornito "*an authoritative attempt to clarify and formulate rules of law governing the use of aircraft in war*".[760]

2.2. Le Convenzioni di Ginevra del 1949 ed il I Protocollo Addizionale

L'Art. 46 del I Protocollo Addizionale del 1977 (IPA) segue la traccia delle codificazioni precedenti:

> *Nonobstant toute autre disposition des Conventions ou du présent Protocole, un membre des forces armées d'une Partie au conflit qui tombe au pouvoir d'une Partie adverse alors qu'il se livre à des activités d'espionnage n'a pas droit au statut de prisonnier de guerre et peut être traité en espion.*[761]

Il primo paragrafo riconferma senza particolari variazioni i principi ormai noti: la spia caduta nelle mani del nemico non ha diritto allo status di prigioniero di guerra, pur essendo espressamente ricompresa tra i membri delle forze armate ("*un membre des forces armées*"). Tale differenza di trattamento ha portato la dottrina a collocare la spia, così come i sabotatori ed i mercenari, nella categoria dei cd. "combattenti non privilegiati".[762]

Come si può notare, non è indicato un criterio utile a distinguere l'*espion* dal legittimo combattente. La lacuna è colmata dal paragrafo successivo, che consente di estrapolare una definizione *a contrario*:

> *Un membre des forces armées d'une Partie au conflit qui recueille ou cherche à recueillir, pour le compte de cette Partie, des renseignements dans un territoire contrôlé par une Partie adverse ne sera pas considéré comme se livrant à des activités d'espionnage si, ce faisant, il est revêtu de l'uniforme de ses forces armées.*[763]

---

terre"; Ibidem, Art. 29: "*La répression des faits d'espionnage visés aux articles 27 et 28 est soumise aux articles 30 et 31 du Règlement concernant les lois et coutumes de la guerre sur terre.*"

[760] L OPPENHEIM, *op. cit.* 519; *cfr.* http://www.icrc.org/ihl/INTRO/275?OpenDocument.

[761] *I Protocole Additionnel* 1977, Art. 46(1).

[762] RONZITTI N., *Diritto Internazionale dei Conflitti Armati* (Giappichelli, 4a edn, 2011) 227.

[763] I Protocollo Addizionale del 1977, Art. 46(2).

Coerente con la tradizione normativa, il Protocollo sveste dei propri privilegi solo chi non indossi l'uniforme dell'esercito di appartenenza. Che la raccolta di informazioni sia conseguita o tentata, è ininfluente.

Dal testo si evincono due novità rispetto al Regolamento dell'Aia: *in primis*, è mutato il limite di applicazione territoriale ("*dans la zone d'opérations d'un belligérant*").[764] Come si vedrà meglio in seguito, la nuova norma si applica a tutto il territorio controllato dalla parte belligerante, incluse le zone occupate.[765]

In secondo luogo, scompare dall'enunciato l'elemento volitivo, i.e. l'intenzione di comunicare all'avversario le informazioni carpite. Nella disciplina attuale, è sufficiente che la spia agisca per conto ("*pour le compte*") della fazione nemica. La nuova formulazione può avere effetti rilevanti. È possibile ritenere, infatti, che per processare come spia l'individuo catturato sia necessario dimostrare prima di tutto il suo nesso di subordinazione con il nemico.

2.2.1. Lo status di prigioniero di guerra

Pur essendo un metodo di combattimento legittimo, lo spionaggio è ritenuto specialmente pericoloso. Per questo motivo alle parti belligeranti è stato fornito un efficace deterrente: privare la spia dello status di prigioniero di guerra (PdG).[766]

Bisogna specificare che, almeno nella formulazione del I Protocollo Addizionale, si tratta di una mera potestà di chi consegue la cattura: l'Art. 46(1) recita infatti "peut être *traité en espion*" (enfasi aggiunta).[767] La seconda precisazione da fare, è che le previsioni delle prime due Convenzioni di Ginevra del 1949 continuano ad applicarsi in ogni caso qualora la spia sia malata, ferita o naufragata.[768]

---

[764] *Cfr.* Y DINSTEIN, *op. cit.*
[765] ICRC, "Commentary – Spies" *op. cit.* 566 §1775; *Cfr.* R R BAXTER, "So-Called 'Unprivileged Belligerency': Spies, Guerrillas, and Saboteurs" (1951) 28 Brit Y B Int'l L 332: "*In modern warfare, in which even the remotest town is exposed to the danger of attacks by guided missiles, rockets, and parachute troops, the entire territory of a belligerent my with some justice be said to be in a zone of operations. But it is normal to preserve some semblance of distinction between that area and territory which is not subject to military control, if only to provide a line of demarcation between the jurisdiction of the military and civilian authorities*".
[766] ICRC, "Commentary – Spies", *op. cit.* 562 §1768.
[767] *Ibidem*.
[768] *Ibidem*.

Una volta catturato, l'agente operativo è inoltre protetto dalle garanzie (sostanziali e processuali) di cui all'Art. 75 del Protocollo.[769] Si tratta di una disposizione d'ordine generale, che trova applicazione per tutti coloro che "*sont au pouvoir d'une Partie au conflit et qui ne bénéficient pas d'un traitement plus favorable en vertu des Conventions et du présent Protocole*".[770] Il prigioniero deve essere trattato con umanità: non potrà i.a. essere ucciso, sottoposto a umiliazioni, torture o ad altre pene fisiche.[771] Gli è altresì riconosciuto il diritto ad essere informato, in una lingua a lui comprensibile, delle cause della sua cattività.[772] Soprattutto, non può essere pronunciata sentenza (inclusa la condanna a morte) senza un previo processo di fronte ad una corte terza e imparziale, nel rispetto dei principi dell'equo processo generalmente riconosciuti.[773]

In caso d'incertezza circa l'appartenenza o meno del soggetto alla categoria delle spie, questo beneficerà dei privilegi del PdG fintantoché un tribunale competente non si sia pronunciato in merito.[774] In teoria un simile accertamento non dovrebbe presentare particolari difficoltà: una volta appurato che il combattente in questione stava raccogliendo informazioni (o cercava di farlo) per il nemico, l'unico elemento distintivo tra la spia ed il comune militare è l'uniforme. Questo ultimo punto è stato a lungo dibattuto.[775]

Guardando ai lavori preparatori del Protocollo, è possibile concludere che per "*uniforme*" si intende qualsiasi segno distintivo, anche non convenzionale. L'unica condizione essenziale è che il simbolo adottato distingua efficacemente il membro delle forze armate da chi non ne fa parte.[776] La valutazione deve essere operata caso per caso: se le insegne indossate dal combattente sono ingannevoli o sufficientemente ambigue, riceverà il trattamento riservato alla spia. Se l'inganno

[769] È quanto disposto ex Art. 45(3) IPA, primo periodo: "*Toute personne qui, ayant pris part à des hostilités, n'a pas droit au statut de prisonnier de guerre et ne bénéficie pas d'un traitement plus favorable conformément à la IVe Convention a droit, en tout temps, à la protection de l'article 75 du présent Protocole.*"
[770] *I Protocole Additionnel du 1977*, Art. 75(1).
[771] *Ibidem*, Art. 75(2).
[772] *Ibidem*, Art. 75(3).
[773] *Ibidem*, Art. 75(4).
[774] ICRC, "Commentary – Spies", *op. cit.* 562 §1769.
[775] *Ibidem* 566 §1776.
[776] *Ibidem* 566-567 §1776.

degenera nella perfidia, l'avversario potrà lamentare una violazione ex Art. 37(2) IPA.[777]

2.2.2. Spie nei territori occupati

L'Art. 46 IPA detta delle previsioni particolari con riguardo ai territori occupati. Il terzo paragrafo prevede che:

> *Un membre des forces armées d'une Partie au conflit qui est résident d'un territoire occupé par une Partie adverse, et qui recueille ou cherche à recueillir, pour le compte de la Partie dont il dépend, des renseignements d'intérêt militaire dans ce territoire, ne sera pas considéré comme se livrant à des activités d'espionnage, à moins que, ce faisant, il n'agisse sous de fallacieux prétextes ou de façon délibérément clandestine.*
>
> *De plus, ce résident ne perd son droit au statut de prisonnier de guerre et ne peut être traité en espion qu'au seul cas où il est capturé alors qu'il se livre à des activités d'espionnage.*

Rispetto a quanto visto in precedenza, la formulazione presenta delle caratteristiche che rendono il testo molto simile all'Art. 29 del *Règlement de la Haye*. L'efficacia territoriale torna ad essere più circoscritta: "*d'un territoire occupé par une Partie adverse*". Inoltre, va a perdersi il riferimento esplicito all'uniforme, riproponendo la formula "*fallacieux prétextes ou de façon délibérément clandestine*".[778] È dunque lecito ritenere che, in un territorio occupato, le sanzioni previste per lo spionaggio si applichino *de facto* a chiunque abbia agito sotto falsi pretesti o in modo deliberatamente clandestino.[779]

Di contro, ciò significa anche che la semplice mancanza dell'uniforme o comunque di un segno distintivo non è determinante, i.e. non corrisponde necessariamente a "falsi pretesti".[780] Si pensi agli insorti e ai guerriglieri che, per la natura delle ostilità, non possono distinguersi dalla popolazione civile: ex Art. 44(3) IPA essi preservano il proprio status di combattenti a condizione che portino le armi apertamente. Analogamente, si può sostenere che qualora carpiscano

[777] *Cfr*. *Ibidem*.
[778] *Ibidem*, 568 §1778.
[779] *Ibidem*, 568 §1779; *cfr*. *Ibidem* 567 §*1777:* i civili sono espressamente esclusi dalla portata dell'Art. 46(3), che è indirizzato ai soli membri delle *forces armées*.
[780] *Ibidem*.

informazioni (senza indossare segni distintivi ma portando le armi apertamente) non possono essere privati dei privilegi del PdG.[781]

Un'altra peculiarità del paragrafo terzo è quella di restringere la portata oggettiva della norma: le informazioni spiate devono avere un valore militare, o la fattispecie non si considera realizzata. È stato sostenuto che una simile specificazione varrebbe in tutte le situazioni, i.e. non solamente all'interno dei territori occupati.[782]

Il secondo periodo contiene un'ulteriore deroga al regime generale: l'agente deve essere necessariamente colto sul fatto ("*capturé alors qu'il se livre à des activités d'espionnage*"). In questo caso opera una sorta di *fictio juris* per cui, nei territori occupati, la spia residente si considera ricongiunta con la propria fazione non appena abbia concluso l'atto di spionaggio.[783]

L'Art. 46(4) si rivolge invece ai non residenti:

> *Un membre des forces armées d'une Partie au conflit qui n'est pas résident d'un territoire occupé par une Partie adverse et qui s'est livré à des activités d'espionnage dans ce territoire ne perd son droit au statut de prisonnier de guerre et ne peut être traité en espion qu'au seul cas où il est capturé avant d'avoir rejoint les forces armées auxquelles il appartient.*

Specularmente al paragrafo precedente, il testo appena citato richiama il dettato dell'Art. 31 del *Règlement de la Haye*. Il non residente, coerentemente alla disciplina generale, è esente da responsabilità per atti di spionaggio pregressi qualora riesca a ricongiungersi con le forze armate alle quali appartiene. Tuttavia, possono sorgere incertezze intorno alla locuzione "*rejoint les forces armées*"

---

[781] *Ibidem* 568-569 §1779; con riferimento ai membri delle forze armate residenti in territori occupati vd. Rapporteur's Report, O.R. XV, p. 430, CDDH/III/338: "*[they will] almost necessarily in their everyday life come across information of value to the armed forces to which they belong, and this should not make them spies or serve as a pretext for denying them protection as prisoners of war. On the other hand, it was agreed that, if they disguised themselves in order to gain access to secret information or in other ways used false pretences or deliberate clandestine acts in order to obtain such information, they would be spies. For example, the resident who observes military movements while walking along the street or who takes photographs from his residence would not be engaged in espionage; whereas the resident who uses a forged pass to enter a military base or who, if lawfully on the base, illegally brings a camera with him, would be engaging in espionage.*"

[782] ICRC, "Commentary – Spies", *op. cit.* 568 §1778.

[783] *Ibidem*, 569 §1781.

soprattutto se, e.g. nei casi ex Art. 44(3), non si tratti di un vero e proprio esercito.[784]

Si potrebbe ipotizzare che la spia si sia "ricongiunta" in senso proprio solo una volta uscita dalla giurisdizione della potenza occupante, ad esempio rifugiandosi nel territorio dello Stato mandante, in quello di una potenza alleata o neutrale. Questa è sicuramente una delle situazioni abbracciate dall'Art. 46(4), ma non l'unica. È altresì possibile che la fazione cui appartiene la spia si trovi all'interno del territorio occupato dal nemico (e.g. in occasione di un *raid* o di una ricognizione). In questo caso, sebbene la presenza avversaria non incida sulla giurisdizione della potenza occupante, l'agente segreto sarà coperto dalla garanzia dello status di PdG anche qualora raggiunga i propri compagni all'interno della zona sottoposta ad occupazione.[785]

2.3. La consuetudine ed i manuali militari

Sebbene il primo Protocollo Addizionale conti ben 174 Stati parti, è lecito chiedersi quali siano le regole applicabili per tutti quelli che ancora non ne hanno ratificato il testo. Fra questi spiccano gli Stati Uniti e Israele,[786] che pure sono tra le potenze militari più attive.[787]

La risposta è che larga parte delle disposizioni contenute nelle Convenzioni di Ginevra e nei relativi Protocolli sono ricognitive del diritto consuetudinario vigente. Lo attesta il Comitato Internazionale della Croce Rossa, che in un'opera monumentale ha raggruppato tutte le regole consuetudinarie riconosciute nel DIU.[788] La Regola 107 riguarda lo spionaggio, e afferma che:

---

[784] *Ibidem*, 570 §1782.
[785] *Ibidem*.
[786] ICRC, Risorse Online: http://www.icrc.org/applic/ihl/dih.nsf/Treaty.xsp?documentId=CBEC955A2CE7E0D4C12563140043ACA5&action=openDocument.
[787] *Rectius* gli USA hanno firmato il Protocollo senza però ratificarlo. Lo stesso hanno fatto Pakistan, Iran e Turchia. Lo Stato d'Israele non è neanche tra i firmatari: http://www.icrc.org/applic/ihl/dih.nsf/States.xsp?xp_viewStates=XPages_NORMStatesSign&xp_treatySelected=470.
[788] J M HENCKAERTS & L DOSWALD-BECK, *op. cit.*

Combatants who are captured while engaged in espionage do not have the right to prisoner-of-war status. They may not be convicted or sentenced without previous trial.[789]

Sebbene sia più sintetica nell'esposizione, la norma racchiude tutti i tratti essenziali della disciplina convenzionale. Innanzitutto, la spia non ha diritto allo status di PdG.[790] È stato anche osservato che molti manuali militari nazionali

---

[789] *Ibidem*, 389.

[790] *Ibidem*; *cfr.* Australia, *Commander's Guide* [1994] §707: "*The most notable exception to granting of PW status to enemy military personnel is to those individuals who are classified as spies* […] *Such individuals are not entitled to PW status and may be tried as common criminals under the detaining power's criminal code. It is important to note, however, that if military clothing is worn during such operations, the perpetrators are lawful combatants and are entitled to PW status*"; Belgium, Law of War Manual [1983] 21-22: "*Spying is not contrary to the law of war and, as a result, does not constitute a war crime. Most countries provide, however, that spying is a crime [under domestic law] in order to protect their national interests and the interests of their armed forces. A person who is caught spying for the enemy is liable to punishment, but only after being tried* […] *In general, civilians act as spies. This activity, by itself, does not give them the status of combatant* […] *Members of the armed forces who perform spying missions in the zone of operations will be treated, if captured, either as prisoners of war or as spies, depending on whether they accomplished their mission wearing their uniform or disguised as civilians wearing civilian clothes*"; Cameroon, *Disciplinary Regulation* [1975] Art. 30: "*Members of the Armed Forces in organised units, francs-tireurs detached from their regular units, commando detachments and isolated saboteurs, as well as voluntary militias, self-defence groups and organised resistance formations are lawful combatants on condition that those units, organisations or formations have a designated commander, that their members wear a distinctive sign, notably on their clothing, that they carry arms openly and that they respect the laws and customs of war. These combatants must be considered prisoners of war. Anyone who does not comply with these conditions may be considered a spy subject to the applicable criminal sanctions*; Cameroon, *Instructors' Manual* [1992] 89: "*[a combatant caught spying] loses his status as a prisoner of war*"; Canada, *LOAC Manual* [1999] 3-4: "*Members of the armed forces engaging in espionage while not in uniform may be treated as spies and lose their entitlement to PW status if they are captured before rejoining the armed forces to which they belong. Spies who are not in uniform are not lawful combatants. If they engage in hostilities, they may be punished for doing so but only after a fair trial affording all judicial guarantees*"; Croatia, *LOAC Compendium* [1991] 65: "*The Occupying Power may impose the death penalty only on inhabitants guilty of espionage, sabotage [and] intentional offences having caused death. However, such offences must have been punishable by death under the law in force in occupied territory before occupation*"; Croatia, *Commanders' Manual* [1992] 31: "*search for information in uniform or without disguise concealing combatant status is legitimate. Spies may be used but they do not have the right to prisoner-of-war status*"; Ecuador, *Naval Manual* [1989] §12.8.1: "*Spying during armed conflict is not a violation of international law. Captured spies are not, however, entitled to prisoner-of-war status. The captor nation may try and punish spies in accordance with its national law. Should a spy succeed in eluding capture and return to friendly territory, liability to punishment terminates. If subsequently captured during some other military operation, the former spy cannot be tried or punished for the earlier act of espionage*"; France, *LOAC Teaching Note* [2000] 2: "*spies […] are not combatants and have no right to prisoner-of-war status*"; France, *LOAC Manual* [2001] 64: "*a spy has no right to prisoner-of-war status and is subject to the national legislation of the territory where he is captured*"; Germany, *Military Manual* [1992] §321-322: "*Even if they are members of their armed forces, [spies] do not have the right to the status of prisoner of war. Persons who fall into the hands of the adversary while engaging in espionage shall be liable to punishment. Even if taken while engaging in espionage, a spy shall not be punished without prior conviction pursuant to regular judicial proceedings*"; Hungary, *Military Manual* [1992] 101: "*The Occupying Power*

may impose the death penalty only on inhabitants guilty of espionage, sabotage [and] intentional offences having caused death. However, such offences must have been punishable by death under the law in force in occupied territory before occupation"; Israel, *Manual on the Laws of War* [1998] 59: "*The spy does not meet the conditions required of a legal combatant (since he is assimilated in the civilian population) and thus is not entitled to the prisoner-of-war's immunity against being tried. Therefore, a state that captures a spy is allowed to bring him to trial in accordance with its own internal laws, an offense that is generally punishable by a long prison sentence or even death* […] *A spy who has succeeded in completing his mission and returning to his army is once again entitled to legal combatant status*"; Italy, *LOAC Elementary Rules Manual* [1991] §31: "*search for information in uniform or without disguise concealing combatant status is legitimate. Spies may be used but they do not have the right to prisoner-of-war treatment*"; Kenya, *LOAC Manual* [1997] Précis 2, 9: "*Those captured while engaged in espionage do not have POW status but may not be punished without trial* […] *Members of the armed forces who were involved in spying cease to be spies as soon as they return to their own lines. If subsequently captured, they cannot be punished for their previous spying activities*"; Madagascar, *Military Manual* [1994] Fiche 5-O §31: "*the search for information in uniform or without disguise concealing combatant status is legitimate. Spies may be used but they do not have the right to prisoner-of-war status*"; Netherlands, *Military Manual* [1993] III-5,III-6: "*A member of the armed forces who falls into the hands of the adversary while engaged in espionage has no entitlement to the status of prisoner of war; he can be treated as a spy* […] *Military spies, who rejoin their forces after having accomplished their task and are subsequently captured, must be treated as prisoners of war and no longer be convicted for their earlier spying activities* […] *A spy caught in the act may under no circumstances be sentenced without trial*"; New Zeland, *Military Manual* [1992] §506(2)(3)(4): "*Although spying is not contrary to the law of armed conflict, international law provides that spies, if captured, may be tried in accordance with the law of the captor and may be liable to the death penalty. To punish them without a proper trial is, however, a war crime. The collection of information by persons wearing uniform is a permitted means of conflict and a person so engaged is liable to be fired upon as is any other member of the enemy forces. If captured, such a person is to be treated as a prisoner of war* […] *Persons who have evaded capture when carrying out acts of espionage and who have rejoined their own forces or own national authority cannot be charged with such acts if subsequently captured; if they are members of armed forces they must be treated as prisoners of war*"; Nigeria, *Manual on the Laws of War* [*undated*] §31: "*For the purpose of waging war it is necessary to obtain information about the enemy. To get such information, it is lawful to employ spies and use soldiers and civilians of the enemy for committing acts of treason. But although this practice by the states is considered legitimate, lawful punishment under the municipal law may be imposed upon individuals engaged in espionage or treason when they are caught by the enemy* […] *Soldiers wearing their uniform when penetrating the enemy zone of operations are not spies and if captured, should be treated as prisoners of war. When a spy is apprehended, he should not be punished without a fair regular trial. A spy who succeeds to rejoin his armed forces and is subsequently captured by the enemy is not liable to be punished for his previous acts of espionage. Such immunity is not accorded to a civilian spy captured by the enemy after reaching his own territory*"; Sweden, *IHL Manual* [1991] 36 §3.2.1.4: "*spies […] are not entitled to combatant or prisoner-of-war status*"; Switzerland [1987] Artt. 41(2), 43: "*International law applicable in armed conflict does not prohibit the use of spies and secret agents, who can even be soldiers or civilians of enemy nationality. Nevertheless, upon their capture or arrest, these persons are liable to be sentenced severely, according to the domestic law of the State concerned* […] *A spy who is caught in the act may not be sentenced without previous judgement*"; United Kingdom, *Military Manual* [] : "*regular members of the armed forces who are caught as spies are not entitled to be treated as prisoners of war. But they would appear to be entitled, as a minimum, to the limited privileges conferred upon civilian spies or saboteurs by [Article 5 GC IV]*"; United Kingdom, *LOAC Manual* [1981] Section III, 9-10 §6: "*Those captured while engaged in espionage do not have PW status but may not be punished without trial. If members of the armed forces gather intelligence in occupied territory they may not be treated as spies provided that they are in uniform. Even if not in uniform, members of the armed forces who were involved in spying cease to be spies as soon as they return to their own lines. If subsequently captured they cannot be punished for their previous spying activities*"; USA, *Naval Handbook* [] : "*Spying during armed conflict is not a violation of international law. Captured spies are not,*

specificano che lo stesso trattamento è riservato ai combattenti sorpresi a compiere atti di spionaggio senza indossare l'uniforme.[791] Non è attestata alcuna prassi ufficiale contraria.

Il secondo periodo della Regola ribadisce il divieto di pronunciare sentenza nei confronti della spia senza un previo processo. Ne consegue che anche e soprattutto in questo caso le esecuzioni sommarie sono proibite.[792]

---

however, entitled to prisoner-of-war status. The captor nation may try and punish spies in accordance with its national law. Should a spy succeed in eluding capture and return to friendly territory, liability to punishment terminates. If subsequently captured during some other military operation, the former spy cannot be tried or punished for the earlier act of espionage"; J M HENCKAERTS & L DOSWALD-BECK, *Customary International Humanitarian Law Volume II: Practice* (Cambridge, 2005) 2563-2565.

[791] J M HENCKAERTS & L DOSWALD-BECK, *Customary International Humanitarian Law Volume I: Rules* (Cambridge, 2009) 389; vd. Argentina, *Law of War Manual* [1989] § 1.09(1); Australia, *Commanders' Guide* [1994] § 707: "*[spies are] combatants who conduct covert espionage operations in enemy occupied territory, while not in uniform*"; Canada, *LOAC Manual* [1999] 3-6, §23-33: "*[espionage is] the collection of information clandestinely behind enemy lines or in the zone of operations while wearing civilian clothing or otherwise disguised or concealed. Spies are those who engage in espionage* […] *[M]embers of the armed forces of a party to the conflict who gather or attempt to gather information while wearing the uniform of their armed forces will not be considered as engaging in espionage*"; Belgium, *Law of War Manual* [1983] 21: "*[a spy is] an individual who gathers or attempts to gather, clandestinely or on false pretences, information in the zone of operations of a belligerent with the intention of communicating it to the adverse party*"; Ecuador, *Naval Manual* [1989] §12.8: "*[a spy is] someone who, while in territory under enemy control or the zone of operations of a belligerent force, seeks to obtain information while operating under a false claim of non-combatant or friendly forces status with the intention of passing that information to an opposing belligerent. Members of the armed forces who penetrate enemy-held territory in civilian attire or enemy uniform to collect intelligence are spies. Conversely, personnel conducting reconnaissance missions behind enemy lines while properly uniformed are not spies*"; Germany, *Military Manual* [1992] §321 : "*[spies are] persons who clandestinely or on false pretences, i.e. not wearing the uniform of their armed forces, gather information in the territory controlled by the adversary*"; Kenya, *LOAC Manual* [1997] 9: "*Soldiers or civilians acting clandestinely or on false pretences to obtain information about a belligerent with the intention to communicate it to his enemy are engaged in espionage* […] *Soldiers wearing their uniform when penetrating the enemy zone of operations are not spies and if captured, should be treated as prisoners of war*"; Spain, *LOAC Manual* [1996] Vol. I §1.4.a: "*a member of the armed forces who gathers information is not considered to be engaged in espionage if that person is wearing regular uniform or is a resident in an occupied territory and is collecting information in that territory on behalf of the occupied power*"; Switzerland, *Basic Military Manual* [1987] Art. 42: "*[a spy is] an individual who, acting clandestinely or on false pretences, gathers or attempts to gather information in the zone of operation of a belligerent with the intention of communicating it to the adverse party*"; United Kingdom, *LOAC Manual* [1981] Section III, 9 §6: "*[spies are] persons who, acting clandestinely or on false pretences, gather information in the territory of a belligerent with intent to communicate it to the enemy*"; USA, *Naval Handbook* [1995] §12.8: "*[a spy is] someone who, while in territory under enemy control or the zone of operations of a belligerent force, seeks to obtain information while operating under a false claim of noncombatant or friendly forces status with the intention of passing that information to an opposing belligerent. Members of the armed forces who penetrate enemy-held territory in civilian attire or enemy uniform to collect intelligence are spies. Conversely, personnel conducting reconnaissance missions behind enemy lines while properly uniformed are not spies*"; J M HENCKAERTS & L DOSWALD-BECK, *Customary International Humanitarian Law Volume II: Practice* (Cambridge, 2005) 2563-2565.

L'opera della Croce Rossa si cura anche di ricercare la prassi degli organi giurisdizionali o quasi-giurisdizionali internazionali. Nonostante la scarsità di fonti, è stata rinvenuta una pronuncia della Commissione EDU[793] in materia di spionaggio in tempo di guerra. Nella causa *Treholt v. Norway* fu dichiarato che l'individuo privato della libertà personale, se sospettato di spionaggio, può essere sottoposto a misure speciali di sorveglianza. Ciononostante, i diritti fondamentali del detenuto non possono per ciò solo essere intaccati.[794]

2.4. Il trattamento della spia – Considerazioni

Il DIU consente che la spia catturata dal nemico, attraverso le modalità ed i limiti descritti finora, sia sottoposta alla giurisdizione ordinaria della parte belligerante nemica. Il presente paragrafo si concentrerà sul momento successivo, i.e. il processo per spionaggio e le tutele riconosciute alla persona che vi sia sottoposta. L'opinione generale è che la spia sia consapevole di prendere parte ad un'attività rischiosa e che dunque ne accetti le conseguenze. Sebbene possa apparire riprovevole dal punto di vista morale, nel DIU lo Stato mandante non ha obblighi giuridici nei confronti della spia catturata, che perciò viene letteralmente "lasciata indietro".

Come evidenziato *supra*, l'Art. 75 IPA garantisce che il procedimento si svolga in modo equo ed imparziale. D'altro canto, è sempre possibile che all'estero l'agente sia sottoposto a tortura, trattamenti inumani e degradanti o alla minaccia della pena capitale.[795] Premesso che l'estrema sanzione non è

---

[792] J M HENCKAERTS & L DOSWALD-BECK, *Customary International Humanitarian Law Volume I: Rules* (Cambridge, 2009) 391.

[793] Si tratta di un organo che, prima dell'entrata in vigore del Protocollo 11, era incaricato di valutare la fondatezza delle cause sottoposte alla CtEDU.

[794] *Treholt v. Norway*, Admissibility Decision [1991] ECiHR 192, 194.

[795] G B DEMAREST, *op. cit.* 338: "*spying is accepted as a part of war, but is recognized as being so dangerous that capital punishment is allowed as a discouragement*"; la pena di morte è prevista anche nei codici di condotta di diversi gruppi armati. Per il codice di condotta del *New People's Army* (NPA) nelle Filippine vd. ICRC, "A Collection of Codes of Conduct Issued by Armed Groups" [2011] (93)822 Int Rev Red Cross 489: "*Point 8. The most severe punishment of expulsion and death shall be imposed on those proven to have committed treachery, capitulation, abandonment of post, espionage, sabotage, mutiny, incitement to rebellion, murder, theft, rape, arson and severe malversation of people's funds*"; per il codice di condotta dei Mujahideen in Afghanistan, vd. M SASSÒLI, A A BOUVIER & A QUINTIN, *How Does Law Protects in War? Cases and Documents Vol. III* (ICRC, 3rd edn) Part II, 3: "*[w]hen a spy is captured, if evidence of espionage is found, the spy will be considered as a perpetrator of social destruction. The Provincial responsible has the power to punish him, exile him, or to prevent him from spying with*

universalmente ripudiata,[796] le restanti pratiche appena menzionate sono categoricamente proibite in forza di norme di *jus cogens* poste a tutela dei diritti umani.[797] La questione assume nuove sfumature: una stessa condotta (i.e. l'inerzia del governo o dei canali diplomatici mentre un connazionale viene deprivato di alcuni diritti fondamentali) sarebbe contemporaneamente in linea con il DIU ed in contrasto con la tutela internazionale dei diritti umani.

La dottrina tradizionale ritiene che tra diritti umani e diritto dei conflitti armati esista un'interrelazione del tipo *lex generalis – lex specialis*. Conseguentemente, nel corso delle ostilità, il DIU prevarrebbe sempre in quanto legge più specifica. Si può portare ad esempio il più essenziale dei diritti umani: il diritto alla vita. Durante un conflitto è possibile, purché non lo si faccia con mezzi illegali, uccidere i combattenti nemici. Persino la morte dei civili è tollerata, purché sia rispettato il principio di proporzionalità.[798] Tra diritti umani e DIU, perciò, non esisterebbe una reale interazione quanto piuttosto una reciproca esclusione.[799] Si tratta di una compartimentalizzazione nata innanzitutto sul piano istituzionale. Nel 1947, nel corso della propria opera di codificazione, la ILC decise di non ammettere il diritto dei conflitti armati tra le materie oggetto di studio.[800] Regolare lo *jus in bello* sarebbe equivalso ad ammettere implicitamente l'inutilità del nuovo assetto dato dalla Carta delle Nazioni Unite allo *jus ad bellum*: "*[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of*

---

appropriate measures. The Imam and his deputy are the only ones who have the power to kill the spy who was arrested. No one else can give him death penalty."

[796] Vd. i.a. CEDU, Protocollo 13; ICCPR, *Second Optional Protocol*, 15 December 1989 (il quale ammette la possibilità di mantenere la pena di morte in tempo di guerra previa specifica riserva); OAS, A-53: *Protocol to the American Convention on Human Rights to Abolish the Death Penalty* (anche in questo caso, è possibile presentare una riserva specifica che trova applicazione in tempo di guerra); *cfr.* A/RES/62/149: *Moratorium on the Use of Death Penalty*.

[797] PUSTORINO P., *Appunti di Tutela Internazionale dei Diritti Umani* (2013) 60ss.

[798] T MERON, "The Humanization of Humanitarian Law" [2000] 94 Am J Int'l L 239-240: "*[u]nlike human rights law, the law of war allows, or at least tolerates, the killing and wounding of innocent human beings not directly participating in an armed conflict, such as civilian victims of lawful collateral damage. It also permits certain deprivations of personal freedom without conviction in a court of law. It allows an occupying power to resort to internment and limits the appeal rights of detained persons. It permits far reaching limitations of freedoms of expression and assembly*"; ILC Yearbook [1949-I] 263-264 §20, 224-225; N PRUD'HOMME, "Lex Specialis: Oversimplifying a More Complex and Multifaceted Relationship?" [2007] 40 Isr L Rev 361.

[799] H KRIEGER, "A Conflict of Norms: the Relationship Between Humanitarian Law and Human Rights Law in the ICRC Customary Law Study" [2006] 11 J Conflict & Sec L 266.

[800] ILC Yearbook [1949-I] 263-264 §20, 224-225; N PRUD'HOMME, *op. cit.* 360.

any state, or in any other manner inconsistent with the Purposes of the United Nations".[801] Parimenti, il Comitato Internazionale della Croce Rossa manteneva le distanze dalla tutela internazionale dei diritti umani, considerata il frutto di un programma meramente politico dell'ONU. Rimanendo coerente ai principi dettati dal proprio statuto, l'organizzazione ginevrina preferiva preservare neutralità ed indipendenza.[802] Basti pensare che la Dichiarazione Universale dei Diritti dell'Uomo e le quattro Convenzioni di Ginevra, pur essendo entrate in vigore a distanza di un anno, sono state redatte in modo completamente autonomo.[803]

È innegabile che i due corpi normativi siano molto differenti tra loro. Innanzitutto hanno radici distinte: le leggi che regolano la guerra sono tra le manifestazioni più antiche del diritto internazionale, mentre i diritti umani sono relativamente "giovani".[804] Ancora, il DIU si applica solo nelle zone di conflitto e nei territori occupati, mentre i diritti umani si estendono ovunque in modo trasversale. Quanto all'efficacia temporale, a lungo si è ritenuto che i diritti umani si applicassero sempre, pur lasciando il passo al DIU nel corso delle ostilità.[805]

Mantenere le due sfere completamente separate, però, si è rivelato poco realistico. Già nel 1953 l'Assemblea Generale invitava al rispetto dei diritti umani durante la guerra di Corea.[806] Lo stesso nel 1956, in occasione dell'invasione sovietica dell'Ungheria.[807] Nel 1967, con lo sguardo rivolto ai territori occupati

---

[801] *Charter of the United Nations* 1945, Art. 2(4).
[802] N PRUD'HOMME, *op. cit.*; H KRIEGER, *op. cit.* 267.
[803] H KRIEGER, *op. cit.*; R KOLB, "The Relationship Between International Humanitarian Law and Human Rights Law" [1998] 80 Int'l L Rev Red Cross 409; *cfr.* R PROVOST, *International Human Rights Law and Human Rights* (Cambridge University Press, 2003).
[804] Sebbene la tutela dei diritti umani si possa far risalire ad un ideale illuminista e giusnaturalista di uguaglianza, la questione è rimasta vincolata al diritto costituzionale (e dunque al dominio riservato degli Stati) per lungo tempo. Solo con la Dichiarazione Universale dei Diritti dell'Uomo viene riconosciuta l'esistenza di diritti *erga omnes*, indivisibili ed irrinunciabili. Vd. C DROEGE, "The Interplay Between International Humanitarian Law and International Human Rights Law in Situations of Armed Conflict" [2007] 40 Isr L Rev 313.
[805] H KRIEGER, *op. cit.* 279*;*
[806] A/RES/804(VIII) [3 December 1953] *On the Treatment of Captured Soldiers and Civilians in Korea by North Korean and Chinese Forces*: "*[the General Assembly] condemns the commission by any governments or authorities of murder, mutilation, torture, and other atrocious acts against captured military personnel or civilian populations, as a violation of rules of international law and basic standards of conduct and morality and as* affronting human rights *and the dignity and worth of human persons*" (enfasi aggiunta); C DROEGE, *op. cit.* 314.
[807] A/RES/1312(XIII) [12 December 1858] *The Situation in Hungary*: "*[the General Assembly] again calls upon the Union of Soviet Socialist Republics* […] *to respect the liberty and political independence of Hungary and the Hungarian people's enjoyment of fundamental rights and freedoms*"; C DROEGE, *op. cit.*

durante la guerra dei sei giorni, il Consiglio di Sicurezza affermò che "*essential and inalienable human rights should be respected even during the vicissitudes of war*". [808] L'anno successivo la *International Conference on Respect and Enforcement of Human Rights in Armed Conflict* invitava Israele ad applicare, nei territori palestinesi, tanto le Convenzioni di Ginevra quanto i diritti umani.[809] Sulla stessa linea, seguì una nuova Risoluzione dell'Assemblea Generale. Questa si intitolava "*Respect for Human Rights in Armed Conflicts*" e riconosceva i.a. "*the necessity of applying basic humanitarian principles in all armed conflicts*". [810] In verità, svariate risoluzioni dal contenuto simile sono state promulgate negli anni tanto dal Consiglio di Sicurezza, che dall'Assemblea Generale e dalla Commissione per i Diritti Umani.[811]

Anche la Croce Rossa, dopo le prime titubanze, si aprì gradualmente al dialogo: la Conferenza Diplomatica tenutasi tra il 1974 ed il 1977[812] dovette riconoscere che *"[h]uman rights continue to apply concurrently [with IHL] in time of armed conflict*".[813]

Se dunque la relazione tra DIU e diritti umani è un dato di fatto, le modalità con cui questi interagiscono erano (e sono) ampiamente dibattute. L'argomento è stato affrontato anche dalla CIG, che nel parere consultivo *Nuclear Weapons*[814] ha negato il tradizionale approccio settoriale:

> *The Court observes that the protection of the International Covenant of Civil and Political Rights does not cease in times of war, except by*

---

[808] S/RES/237 (1967); C DROEGE, *op. cit.* 315.

809 A/CONF 32/41 *Proclamation of Teheran, Final Act of the International Conference on Human Rights*, Teheran, 22 April to 13 May 1968, §10: "*Massive denials of human rights, arising out of aggression or any armed conflict with their tragic consequences, and resulting in untold human misery, engender reactions which could engulf the world in ever growing hostilities. It is the obligation of the international community to co-operate in eradicating such scourges*"; C DROEGE, *op. cit.*

[810] A/RES/2444(XIII) [19 December 1968] *Respect for Human Rights in Armed Conflicts*.

[811] *Cfr*. S/RES/1019 (1995); S/RES/1034 (1995); S/RES/1635 (2005); S/RES/1653 (2006); A/RES/50/193; A/RES/3525(XXX); A/RES/46/135; A/RES/52/145; E/CN.4/1992/84; E/CN.4/2003/77; A/E/CN.4/RES/2003/16; E/CN.4/RES/2001/24; E/CN.4/RES/2003/15; OHCRH/STM/CHR/03/2; HCHR/STM/CHR/03/3; E/CN.4/1992/26; C DROEGE, *op. cit.* 316.

[812] *Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law*, i cui lavori porteranno alla pubblicazione dei primi due Protocolli Addizionali alle Convenzioni di Ginevra.

[813] *Commentary on the Additional Protocols* (Y. Sandoz, C. Swinarski, & B. Zimmermann edn, 1987); C DROEGE, *op. cit.* 316.

[814] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion of 8 July 1996, ICJ Reports 1996(I), ICJ.

operation of Article 4 of the Covenant whereby certain provisions may be derogated from in a time of national emergency. Respect for the right to life is not, however, such a provision. In principle, the right not arbitrarily to be deprived of one's life applies also in hostilities. The test of what is an arbitrary deprivation of life, however, then falls to be determined by the applicable lex specialis*, namely, the law applicable in armed conflict which is designed to regulate the conduct of hostilities. Thus whether a particular loss of life, through the use of a certain weapon in warfare, is to be considered an arbitrary deprivation of life contrary to Article 6 of the Covenant, can only be decided by reference to the law applicable in armed conflict and not deduced from the terms of the Covenant itself.*[815]

La Corte riconduce il rapporto tra i due impianti normativi alla *lex specialis*, ma assume al tempo stesso una posizione nuova: nei conflitti armati il DIU non esclude necessariamente la tutela dei diritti umani.

Questa linea giurisprudenziale è ulteriormente sviluppata nell'opinione riguardante la costruzione di un muro in Palestina:[816]

the Court considers that the protection offered by human rights conventions does not cease in case of armed conflict, save through the effect of provisions for derogation of the kind to be found in Article 4 of the International Covenant on Civil and Political Rights. As regards the relationship between international humanitarian law and human rights law, there are thus three possible situations: some rights may be exclusively matters of international humanitarian law; others may be exclusively matters of human rights law; yet others may be matters of both these branches of international law. In order to answer the question put to it, the Court will have to take into consideration both these branches of international law, namely human rights law and, as lex specialis*, international humanitarian law.*[817]

---

[815] *Ibidem*, 239 §25.
[816] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion of 9 July 2004, ICJ.
[817] *Ibidem*, §106.

La Corte è ancora restia ad abbandonare il criterio della *lex specialis*, eppure nel caso di specie riconosce l'esistenza di tre scenari distinti:

1) Situazioni in cui la questione riguarda unicamente il diritto umanitario.
2) Situazioni concernenti solamente i diritti umani.
3) Situazioni in cui le due categorie precedenti si rivelano complementari e che meritano una valutazione caso per caso.

Se quindi la CIG in questa sede ha già superato *de facto* l'impostazione tradizionale, solo un anno più tardi abbandonerà definitivamente ogni riferimento formale alla *lex specialis* nella decisione *DRC v. Congo*.[818] Rievocando la precedente giurisprudenza sui rapporti tra diritti umani e DIU, la Corte ripresentò il passaggio appena estrapolato dalla opinione *Wall in Palestine*. Tuttavia, dal testo citato fu espunta la formulazione "*as* lex specialis".[819] Una simile omissione può essere considerata casuale, oppure si può ritenere che la Corte abbia preso coscienza del fatto che la *lex specialis* non rispecchia completamente l'attuale situazione giuridica.

Anche sul piano normativo la complementarietà tra queste due branche del diritto internazionale è ormai una realtà. Diversi strumenti convenzionali fanno esplicito richiamo ad entrambe, rendendone necessaria l'interrelazione: la Convenzione Internazionale sui Diritti del Fanciullo (1989)[820] ed il relativo protocollo opzionale del 2000,[821] lo Statuto di Roma della Corte Penale Internazionale (2002), i *Basic Principles and Guidelines on the Right to a Remedy*

[818] *Case Concerning Armed Activities on the Territory of the Congo (DRC v. Uganda)* of 19 December 2005, ICJ, §216.
[819] *Ibidem*: "*The Court first recalls that it had occasion to address the issues of the relationship between international humanitarian law and international human rights law and of the applicability of international human rights law instruments outside national territory in its Advisory Opinion of 9 July 2004 on the* Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory. *In this Advisory Opinion the Court found that "the protection offered by human rights conventions does not cease in case of armed conflict, save through the effect of provisions for derogation of the kind to be found in Article 4 of the International Covenant on Civil and Political Rights. As regards the relationship between international humanitarian law and human rights law, there are thus three possible situations: some rights may be exclusively matters of international humanitarian law; others may be exclusively matters of human rights law; yet others may be matters of both these branches of international law." It thus concluded that both branches of international law, namely international human rights law and international humanitarian law, would have to be taken into consideration*"; N PRUD'HOMME, *op. cit.* 385.
[820] Vd. Art. 38: "Gli Stati parti s'impegnano a rispettare ed a garantire il rispetto delle norme di diritto internazionale umanitario applicabili nei casi di conflitto armato e la cui tutela si estenda ai fanciulli"; C DROEGE, op. cit. 508.
[821] A/RES/54/263 (12 February 2002); C DROEGE, op. cit.

and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law (2006),[822] nonché la Convenzione delle Nazioni Unite sui Diritti delle Persone con Disabilità (2006).[823]

Riassumendo, il concetto di *lex specialis* implica esclusività: obbliga a scegliere, in un dato contesto, se applicare i diritti umani od il diritto dei conflitti armati. Alla luce di quanto sostenuto finora, pare che l'approccio da preferire sia piuttosto quello di valutare ogni diversa situazione ed applicare tanto il DIU quanto i diritti umani in modo opportuno e bilanciato.

Assumendo perciò che la spia catturata dal nemico goda ancora del proprio diritto ad essere trattata con umanità, a non essere torturata, finanche a non essere condannata a morte, resta da vedere quali siano gli strumenti esistenti per garantirle un'efficace godimento di tali diritti. Si tratta del punto più problematico della questione, dal momento che l'agente catturato è ormai soggetto alla giurisdizione di uno Stato straniero. Non solo: è pure possibile che lo Stato nazionale della spia abbia abolito la pena di morte in forza di una convenzione internazionale, mentre nell'ordinamento giuridico della parte avversaria la pena capitale sia legittima. In questo caso, si può ipotizzare una responsabilità dello Stato nazionale della spia affinché si attivi quantomeno sul piano delle relazioni internazionali. Di seguito vengono proposte due opzioni.

Qualora entrambi i belligeranti siano parti del Patto sui Diritti Civili e Politici, ci si può augurare che lo Stato nazionale della spia attivi una *complaint procedure* dinanzi al Comitato, lamentando una violazione dell'Art. 7.[824]

La giurisprudenza della CtEDU offre uno spunto ulteriore. Nel caso *Soering*,[825] la Corte concluse che un cittadino tedesco non poteva essere estradato negli Stati Uniti dove avrebbe vissuto in condizioni inumane e degradanti nel braccio della morte.[826] La Corte riconosceva dunque in capo ai membri del CdE

[822] A/RES/60/147 (21 March 2006); C DROEGE, op. cit.
[823] A/RES/61/106 (13 December 2006); C DROEGE, op. cit.
[824] ICCPR, Art. 7: "*No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment. In particular, no one shall be subjected without his free consent to medical or scientific experimentation*"; per le modalità della *complaint procedure* vd. *supra* §2.1.2; ICCPR, Art. 41.
[825] *Soering v. United Kingdom* (Application no 14038/88) [1989] CEDU.
[826] *Ibidem*, §111.

un obbligo positivo di prevenire la violazione di diritti fondamentali garantiti dalla CEDU (l'Art. 3 nel caso di specie) anche se ad agire in concreto sia uno Stato terzo non firmatario. Tra l'altro dopo il 2002, in forza del XIII Protocollo Addizionale alla CEDU, si deve ritenere che per gli Stati ratificanti non sia più possibile l'estradizione verso paesi che prevedono la pena di morte, fosse anche solo in tempo di guerra.[827]

L'ipotesi della spia catturata dal belligerante nemico presenta ovviamente delle differenze rispetto al caso *Soering*, se non altro perché l'agente non è in procinto di essere estradato, ma è già detenuto nel territorio della fazione avversaria. Ciò comporta una capacità d'azione molto più limitata per lo Stato nazionale della spia, ma non per questo vengono meno gli obblighi imposti dalla tutela internazionale dei diritti umani. Si può auspicare che in questa particolare situazione si agisca in protezione diplomatica, sempreché i relativi canali (ambasciate, consolati, rappresentanze all'estero) non siano stati interrotti in ragione del conflitto in corso. Non solo: in linea con un'applicazione "pratica ed effettiva"[828] della CEDU, potrebbe configurarsi un vero e proprio obbligo per lo Stato membro di fornire la propria protezione diplomatica in situazioni come quella appena descritta, e di riflesso un diritto dell'individuo ad essere assistito.

[827] Lo stesso principio è stato codificato dalla Carta di Nizza all'Art. 19(2).
[828] *Artico v. Italy* (Application no 6694/74) [1980] CEDU: "*The Court recalls that the Convention is intended to guarantee not rights that are theoretical or illusory but rights that are practical and effective*".

CAPITOLO IV: L'*INTELLIGENCE* IN ITALIA

1. L'Italia dopo *datagate* – Il Garante della Privacy

Anche in Italia lo scandalo *datagate* ha avuto le proprie ripercussioni. Nonostante le prime smentite da parte delle autorità all'indomani dell'inchiesta di Glenn Greenwald,[829] oggi sembrano non esserci dubbi sul fatto che anche i cittadini italiani siano caduti nella rete dell'*intelligence* statunitense.[830]

In qualità di Stato membro dell'Unione Europea e del Consiglio d'Europa, l'Italia condivide con i paesi del vecchio continente i principi fondamentali su cui si regge l'*acquis* posto a tutela di *privacy* e dati personali. Conformemente alla Direttiva 95/46/CE e alla Convenzione 108, nel nostro ordinamento il trattamento di dati per motivi di sicurezza nazionale deve essere previsto *ex lege* e non arbitrario. Nel contemperamento tra *privacy* e libertà, il cittadino è sempre privilegiato. L'eccezionale ingerenza dei pubblici poteri, perciò, deve essere necessaria e proporzionata.

Nelle prossime pagine verrà illustrato come il legislatore abbia recepito la Direttiva del '95 e soprattutto quale sia il ruolo della nostra autorità di controllo (il cd. Garante della *privacy*) di fronte alle sfide giuridiche provenienti da oltreoceano. Il secondo passo sarà quello di esaminare l'assetto istituzionale delle agenzie di informazione per la sicurezza della Repubblica, con particolare attenzione alle garanzie di trasparenza che queste offrono ai cittadini nello svolgimento dei propri compiti.

1.1. Il recepimento della Direttiva 95/46/CE in Italia

In Italia il primo strumento attuativo della Direttiva comunitaria fu la l. 675/1996. Si trattava di uno strumento incompleto, che se da una parte ebbe il pregio di riconoscere efficacemente il diritto alla riservatezza, presentava ancora

[829] RONZITTI N., *Il Caso Snowden e le Regole dello Spionaggio* in IAI Rivista Online, 2013: http://www.affarinternazionali.it/articolo.asp?ID=2369.
[830] Secondo la stampa, in Italia sarebbero stati raccolti circa 46 milioni di metadati riguardanti conversazioni telefoniche.

diverse lacune che la distanziavano dagli standard europei.[831] È con il d.lgs. 196/2003, intitolato "Codice di protezione dei dati personali", che la materia viene adeguata e riformata, anche alla luce della Carta di Nizza.[832]

La nuova normativa punta ad una "più incisiva tutela della persona umana nel rispetto dei diritti e delle libertà fondamentali dell'interessato, nonché della sua dignità".[833] Soprattutto, è interessante notare come il diritto alla protezione dei dati personali sia riconosciuto a "chiunque",[834] senza alcun accenno a deroghe, discriminazioni o distinzioni tra cittadini italiani e non cittadini. Si tratta della prima e più rilevante differenza tra l'approccio italiano e quello statunitense.

Il Codice *privacy*, inoltre, pone rimedio ad una grave mancanza della legge che l'ha preceduto, introducendo all'Art. 3 il principio di necessità:

> [i] sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.[835]

Tale principio integra quello di pertinenza e non eccedenza di cui all'Art. 11.[836] Si tratta di una disposizione che rispecchia perfettamente la disciplina comunitaria: i

---

[831] *Cfr.* RASI G., *Il nuovo codice sulla protezione dei dati personali tutela la dignità della persona*, 4 Novembre 2004: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/106024.

[832] *Ibidem*.

[833] *Ibidem*, *cfr*. d.lgs. 196/2003, Art. 2(1): "Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".

[834] D.lgs. 196/2003, Art. 1.

[835] *Cfr.* RUSSO S., *Manuale di Diritto Comunitario dell'Informatica* (Giuffrè, edn, 2010), 66.

[836] D.lgs. 196/2003, Art. 11(1): "I dati personali oggetto di trattamento sono:
a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
c) esatti e, se necessario, aggiornati;
d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
e) conservati in una forma che consenta l'identificazione del Codice in materia di protezione dei dati personali l'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati."

dati personali devono essere trattai correttamente ed in modo lecito.[837] Lo scopo del trattamento deve sempre essere determinabile *ex ante* ed i dati devono essere successivamente utilizzati in modo conforme alle finalità dichiarate.[838]

I diritti sostanziali dell'interessato possono ricondursi a tre tipologie:[839]

1) Conoscere se un determinato trattamento ha avuto inizio;
2) Verificare la qualità dei dati trattati e conseguentemente richiederne la rettifica o la cancellazione;
3) Opporsi al trattamento sulla base di motivi legittimi.

Ex Art. 13 è previsto anche che all'interessato sia sempre inoltrata un'informativa completa[840] in modo tale da permettergli di prestare il proprio consenso, libero e cosciente, al trattamento. Ovviamente sono previste eccezioni per agevolare l'esercizio di funzioni "ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati".[841] Cionondimeno, i principi di legalità e necessità non sono derogati neppure in questo caso.

L'Art. 58 è dedicato specificamente al rapporto intercorrente tra Codice *privacy* e organismi preposti alla difesa e alla sicurezza dello Stato.[842] Il primo comma presenta un elenco tassativo degli articoli che devono essere rispettati anche dalle agenzie di *intelligence* del nostro governo quando trattano dati

---

[837] RUSSO S., *op. cit.* 67; CIRILLO G. P., *Il Codice sulla protezione dei dati personali* (Giuffrè, Milano, 2004) 32ss.
[838] *Ibidem*.
[839] RUSSO S., *op. cit.* 70; CIRILLO G. P., *op. cit.* 38.
[840] D.lgs. 196/2003, Art. 13(1): "L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:
a) le finalità e le modalità del trattamento cui sono destinati i dati;
b) la natura obbligatoria o facoltativa del conferimento dei dati;
c) le conseguenze di un eventuale rifiuto di rispondere;
d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
e) i diritti di cui all'articolo 7;
f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile."
[841] D.lgs. 196/2003, Art. 13(2).
[842] *Cfr.* D.lgs. 196/2003, Art.58(1). Il riferimento alla l. 801/1977 deve considerarsi obsoleto, dato che la legge in questione è stata abrogata ex Art. 44(1) della l. 124/2007. Per maggiori approfondimenti, vd. *infra*.

personali (mentre tutti gli altri sono disapplicati *en bloc*). Osservando tale novero si desume che nei confronti dei servizi segreti l'interessato non possa esercitare i propri diritti sostanziali di accesso e opposizione.[843] Tuttavia restano sempre validi i principi fondamentali del Codice, nonché le misure minime di sicurezza in esso previste.[844]

In conformità con l'Art. 28 della Direttiva 95/46/CE,[845] il Codice mantiene operativa l'autorità di controllo istituita dalla l. 675/1996 e denominata "Garante per la protezione dei dati personali" (cd. Garante della *privacy*).[846] Nel paragrafo seguente verranno analizzate le sue funzioni ed il ruolo che questa ha avuto sul fronte italiano del *datagate*.

1.2. Continua – Il Garante della Privacy

Il Garante è un organo collegiale composto da esperti di diritto dell'informatica, eletti di concerto dalle due Camere assicurandone piena autonomia ed indipendenza.[847] A loro volta i componenti del collegio nominano un presidente il cui voto prevale in caso di parità e che dirige i lavori dell'organo istituzionale.[848]

La funzione primaria del Garante è di controllo: si occupa in via preventiva di diffondere una "cultura della *privacy*" attraverso iniziative pubbliche, propone linee guida al Governo e alle Camere, esprime pareri non vincolanti, prescrive ai soggetti responsabili del trattamento le misure necessarie a conformarsi al Codice o vieta loro i trattamenti illeciti. Su base annuale redige una relazione relativa allo stato di attuazione del d.lgs. 196/2003, che viene poi trasmessa alle Camere e al Governo.[849]

---

[843] Gli Artt. 7-10 non figurano nella lista ex Art. 58(1).
[844] *Cfr.* d.lgs. 2003/196, Art. 58(1): "le disposizioni del presente codice si applicano limitatamente a quelle previste negli articoli da 1 a 6, 11, 14 e 15, 31, 33 […]". Come illustrato *supra*, l'Art. 3 codifica il principio di necessità, l'Art. 11 postula liceità e legittimità del trattamento.
[845] "Ogni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare, nel suo territorio, l'applicazione delle disposizioni di attuazione della presente direttiva, adottate dagli Stati membri".
[846] Vd. D.lgs. 2003/196, Art. 153.
[847] *Ibidem*, Art. 153(2).
[848] *Ibidem*, Art. 153(3); dal 2012 il presidente in carica è Antonello Soro: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1902449.
[849] *Ibidem*, Art. 154.

È dalla relazione per l'anno 2013 che si intuiscono gli sforzi compiuti dal Garante a seguito delle rivelazioni di Snowden, concretizzati in "una serie di attività informative e di impulso nei confronti del Governo, al fine di minimizzare i rischi per i cittadini italiani rispetto ad eventuali acquisizioni dei loro dati per fini di *intelligence*."[850] Già il 23 Luglio 2013 il Garante veniva audito ex Art. 31(3) della l. 124/2007 dal Copasir,[851] al fine di comprendere l'estensione del programma di *bulk data collection* in Italia. Veniva contestualmente riesaminato il rapporto esistente tra *privacy* e sicurezza nel nostro ordinamento.[852]

Il 22 Ottobre 2013 il presidente Soro inviava al Presidente del Consiglio in carica, Enrico Letta, una lettera che lo esortava a promuovere il progetto di riforma europeo sulla *privacy*.[853] La sorveglianza indiscriminata da parte delle agenzie statunitensi era al centro delle preoccupazioni di Soro, che incalzava:

> [i]l problema delle attività di spionaggio della NSA rende indispensabile che il Governo accerti, con tutti gli strumenti utili, se la raccolta, l'utilizzo e la conservazione di informazioni relative alle comunicazioni telefoniche e telematiche abbia coinvolto anche i cittadini italiani.
>
> Si tratta di una indispensabile operazione di trasparenza in quanto tali condotte, se confermate, avrebbero primariamente violato i principi fondamentali in materia di riservatezza dei cittadini e reso evidenti le debolezze connesse alla sicurezza delle reti e dei sistemi informatici rilevanti sul piano nazionale.[854]

Contestualmente il Garante poneva l'accento sulle lacune esistenti nell'ambito dei "trattamenti effettuati per fini di giustizia, polizia o sicurezza nazionale".[855] Infatti, fermo quanto osservato nel paragrafo precedente, è innegabile che le problematiche attuali richiedano un intervento legislativo ben più specifico di quello rinvenibile all'Art. 58 del Codice *privacy*.

---

[850] Garante per la protezione dei dati personali, *La protezione dei dati nel cambiamento: Big Data Trasparenza Sorveglianza – Relazione 2013*, 95: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3182545.
[851] Per maggiori informazioni, vd. *infra*.
[852] Garante per la protezione dei dati personali, *La protezione dei dati nel cambiamento: Big Data Trasparenza Sorveglianza – Relazione 2013*, 95.
[853] Si tratta del "pacchetto *privacy*" di cui al Capitolo II.
[854] SORO A., *Lettera di Antonello Soro al Presidente del Consiglio dei Ministri, Enrico Letta* [22 Ottobre 2013]: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2708275.
[855] *Ibidem*.

Il passo più significativo in questo senso risale al Novembre 2013, quando il Garante ha siglato un protocollo d'intenti con il DIS (Dipartimento delle Informazioni per la Sicurezza dello Stato).[856] Si tratta di un'iniziativa senza precedenti nell'Unione Europea,[857] il cui fine precipuo è la leale collaborazione e la trasparenza tra i due organi amministrativi. Tale scopo è perseguito attraverso "modalità di informazione idonee a consentire al Garante di conoscere alcuni elementi essenziali del trattamento dei dati personali effettuato dagli Organismi per l'informazione e la sicurezza in alcuni contesti peculiari, segnatamente quelli concernenti la sicurezza cibernetica o gli accessi alle banche dati delle pp.aa. o degli esercenti servizi di pubblica utilità".[858] In sintesi, il Garante si affianca al Copasir e all'autorità giudiziaria svolgendo controlli stringenti sulle agenzie italiane di *intelligence* ogniqualvolta accedano alle banche dati di amministrazioni pubbliche, gestori di servizi di pubblica utilità o di servizi inerenti la "sicurezza cibernetica".[859]

La seconda parte del protocollo illustra le modalità attraverso cui il Garante svolgerà i propri accertamenti: il DIS e le Agenzie di Informazione dovranno trasmettere un piano ricognitivo di tutti gli archivi informatici ai quali hanno accesso ex Art. 13(2) della l. 124/2007,[860] nonché dei dati acquisiti ex Art. 11 DPCM 24 Gennaio 2013, [861] laddove abbiano portato all'identificazione

[856] Vd. Garante per la protezione dei dati personali, *La protezione dei dati nel cambiamento: Big Data Trasparenza Sorveglianza – Relazione 2013*, 95.
[857] SORO A., *Big Data Trasparenza Sorveglianza – Relazione 2013: Discorso del Presidente* [10 Giugno 2014] 6-7.
[858] Garante per la protezione dei dati personali, *La protezione dei dati nel cambiamento: Big Data Trasparenza Sorveglianza – Relazione 2013*, 95.
[859] DPCM 24 Gennaio 2013, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, Art. 2(1)(i): "sicurezza cibernetica: condizione per la quale lo spazio cibernetico risulti protetto grazie all'adozione di idonee misure di sicurezza fisica, logica e procedurale rispetto ad eventi, di natura volontaria od accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi".
[860] L. 124/2007, Art. 13(2): "[c]on apposito regolamento, adottato previa consultazione con le amministrazioni e i soggetti interessati, sono emanate le disposizioni necessarie ad assicurare l'accesso del DIS, dell'AISE e dell'AISI agli archivi informatici delle pubbliche amministrazioni e dei soggetti che erogano, in regime di autorizzazione, concessione o convenzione, servizi di pubblica utilità, prevedendo in ogni caso le modalità tecniche che consentano la verifica, anche successiva, dell'accesso a dati personali".
[861] DPCM 24 Gennaio 2013: "Gli operatori privati che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo, il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici, ivi comprese quelle individuate ai sensi dell'art. 1, comma 1, lett.

dell'interessato (i.e. dell'individuo sorvegliato). Per non pregiudicare le operazioni dei servizi segreti, il Garante è tenuto ad assicurare la massima riservatezza dei dati ricevuti.

L'intesa, coerente con il principio di leale collaborazione cui si ispira, prevede anche che il comparto *intelligence* si avvalga dell'attività consultiva del Garante (fuori dei casi già previsti dalla normativa vigente) circa il corretto trattamento dei dati personali. Entrambe le parti nominano uno o più referenti, che hanno il compito di vegliare sull'effettiva applicazione dell'accordo. Quest'ultimo ha durata biennale, ma le parti hanno espresso fiducia in futuri aggiornamenti, soprattutto alla luce dei prevedibili sviluppi normativi e regolamentari in materia.

L'azione del Garante è proseguita anche su un diverso fronte. Come previsto ex Art. 154(2)(h) del Codice *privacy*, il presidente Soro ha premuto sulla sensibilizzazione del pubblico attraverso interviste e comunicati stampa.[862] L'obiettivo è stato e continua ad essere quello di garantire agli utenti della rete una fruizione più serena del Web, nonostante il forte allarme sociale scatenato dall'*affaire* Snowden. Allo stesso tempo è stata ribadita con decisione l'importanza dei dati immessi *online*, i quali possono incidere drasticamente sulla vita e sulla libertà della persona.

Anche sul piano internazionale il Garante ha avuto un ruolo trainante, *in primis* esortando in più occasioni il Governo all'adozione del nuovo Regolamento

---

d), del decreto del Ministro dell'interno 9 gennaio 2008, secondo quanto previsto dalla normativa vigente, ovvero previa apposita convenzione:
a) comunicano al Nucleo per la sicurezza cibernetica, anche per il tramite dei soggetti istituzionalmente competenti a ricevere le relative comunicazioni ai sensi dell'art. 16-bis, comma 2, lett. b), del decreto legislativo n. 259/2003, ogni significativa violazione della sicurezza o dell'integrità dei propri sistemi informatici, utilizzando canali di trasmissione protetti; b) adottano le best *practices* e le misure finalizzate all'obiettivo della sicurezza cibernetica, definite ai sensi dell'art. 16-bis, comma 1, lett. a), del decreto legislativo n. 259/2003, e dell'art. 5, comma 3, lett. d), del presente decreto; c) forniscono informazioni agli organismi di informazione per la sicurezza e consentono ad essi l'accesso alle banche dati d'interesse ai fini della sicurezza cibernetica di rispettiva pertinenza, nei casi previsti dalla legge n. 124/2007; d) collaborano alla gestione delle crisi cibernetiche contribuendo al ripristino della funzionalità dei sistemi e delle reti da essi gestiti."

[862] Vd. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2965259; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3043767; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3127319; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3174869; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3267468; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3370180.

europeo in materia di *privacy* e dati personali.[863] In modo altrettanto significativo, il 10 Settembre 2013 Soro accoglieva Frank La Rue.[864] Nell'ambito del rapporto commissionato dall'Assemblea Generale delle Nazioni Unite,[865] lo *special rapporteur* è stato messo a parte del quadro giuridico italiano con specifico riferimento al delicato equilibrio tra *privacy* e libertà d'espressione.[866] Anche le preoccupazioni scaturite dal *datagate* hanno trovato spazio nella discussione successiva, in particolare per ciò che concerne le nuove forme di *mass surveillance* informatica e telematica.[867]

2. Agenzie di *intelligence* italiane – AISE e AISI

Se fino a questo momento si è fatto riferimento in più occasioni al "comparto *intelligence*" italiano e alla l. 124/2007, ancora non sono state illustrate le caratteristiche fondamentali dei servizi segreti nel nostro paese. I prossimi paragrafi saranno dedicati alla struttura amministrativa dell'*intelligence*: il riparto delle funzioni tra DIS, AISE, AISI ed i principi che guidano il loro operato.

2.1. La legge 124/2007 ed il SIS

La l. 124/2007[868] riforma in modo coeso ed organico la struttura instaurata dalla precedente l. 801/1977.[869] Si tratta del frutto di un lungo iter parlamentare, intrapreso all'indomani della caduta del muro di Berlino. Già il disegno di legge D'Alema – Mattarella[870] del 1999 mostrava un assetto innovativo, che si adattava ad un contesto internazionale profondamente mutato:[871] lo spionaggio militare ed

[863] *Ibidem*.
[864] Vd. Capitolo II *supra*.
[865] Vd. *supra* A/RES/68/167.
[866] Garante per la protezione dei dati personali, *La protezione dei dati nel cambiamento: Big Data Trasparenza Sorveglianza – Relazione 2013*, 192.
[867] *Ibidem*.
[868] Legge 3 Agosto 2007 n. 124, Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto.
[869] Vd. MOSCA C., SCANDONE G., GAMBACURTA S., VALENTINI M., *I servizi di informazione e il segreto di Stato*, Giuffré, Milano, 2008, 23-26: fin dal momento della sua attuazione, l'architettura normativa previgente era stata oggetto di valutazioni critiche e progetti di riforma. D'altro canto, il testo del '97 ebbe il merito di regolare per la prima volta con legge ordinaria una materia fondamentale per la sicurezza dello Stato.
[870] A.S. 4162: http://www.senato.it/leg/13/BGT/Schede/Ddliter/11148.htm.
[871] BIANCO E., *Così è cambiata l'intelligence in Italia* in 3 Gnosis, Rivista Italiana di Intelligence, 2007, 1-2.

il controspionaggio (giunti all'acme durante la Guerra Fredda) cedevano il passo all'esigenza di contrastare la criminalità organizzata ed il terrorismo internazionali.[872] Nonostante gli avvenimenti dell'11 Settembre 2001 acuissero la spaccatura con il passato, gli sforzi riformisti del Senato non trovavano un'adeguata volontà politica alla Camera.[873] Solo durante la XV legislatura (non senza l'impulso di alcune vicende giudiziali che avevano coinvolto i servizi segreti)[874] il nuovo testo fu approvato.

Tale legge istituisce il "Sistema di informazione per la sicurezza della Repubblica" (SIS),[875] un'amministrazione unitaria dell'*intelligence* guidata dal Presidente del Consiglio dei Ministri. Si abbandona la precedente cogestione divisa tra Ministro della Difesa e dell'Interno: il premier assume "l'alta direzione e la responsabilità generale della politica dell'informazione per la sicurezza".[876] Parimenti scompaiono le agenzie SISMi e SISDe, i cui compiti erano suddivisi in base alla natura dell'interesse da tutelare: militare o afferente alla sicurezza nazionale.[877] I nuovi "servizi di informazione per la sicurezza",[878] AISE e AISI, vedono le proprie attribuzioni ripartite secondo un criterio geografico (rispettivamente: minacce esterne e interne).[879] Pur preservando un sistema "binario" di *intelligence*, sono diminuiti drasticamente i problemi di coordinamento tra le due Agenzie. Infatti, alla loro direzione unitaria è stato preposto il Dipartimento delle Informazioni per la Sicurezza (DIS).[880]

Cercando di schematizzare la complessa struttura del SIS, più che ad una piramide si può pensare ad un prisma dalle molte sfaccettature. Al vertice si trova il Presidente del Consiglio, cui spetta i.a. la direzione generale dei servizi segreti

---

[872] A.S. 1513; MOSCA C., *op. cit.* 31: "[i]l consolidarsi di organizzazioni criminali transnazionali che assumono, in contesti geopolitici vulnerabili, crescenti porzioni di potere politico ed economico, l'emergere di pericoli per la sicurezza su terreni del tutto nuovi legati alle risorse, naturali ed energetiche, ai fenomeni migratori, all'ambiente, rappresentano ulteriori indicatori di scenario di un nuovo mondo, globalizzato e tecnologico, in cui si percepisce come il diritto alla sicurezza giochi sul terreno della centralità dell'informazione una partita per molti versi decisiva".
[873] BIANCO E., *op. cit.* 3; MOSCA C., *op. cit.* 26-27.
[874] *Ibidem*, 1; GIUPPONI T. F., *Servizi di informazione e segreto di Stato nella legge n. 124/2007* in www.forumcostituzionale.it.
[875] L. 124/2007, Art. 2.
[876] *Ibidem*, Art. 1(1)(a).
[877] BIANCO E., *op. cit.* 4.
[878] L. 124/2007, Art. 2(2).
[879] *Ibidem*, Artt. 6-7.
[880] *Ibidem*, Art. 4.

italiani, la nomina delle più alte cariche di DIS, AISE e AISI, il loro coordinamento e l'apposizione del segreto di Stato.[881] Attraverso tale assetto unitario, il legislatore della riforma ha perseguito il fine primario dell'effettività e della tempestività nel momento decisionale.[882]

Alle dirette dipendenze del Premier si trova (generalmente) un'Autorità Delegata. Si tratta di una figura introdotta dalla prassi ex Art. 10 della l. 400/1988 ed oggi espressamente prevista dalla nuova legge. All'Autorità vengono attribuite in via non esclusiva funzioni di direzione e coordinamento dei servizi segreti, *en bloc* o a mezzo di specifiche direttive. Il Presidente può in ogni momento avocare a sé l'esercizio delle funzioni delegate.[883]

Il DIS risponde direttamente al Presidente del Consiglio (o all'Autorità Delegata, se presente) nei confronti del quale svolge una funzione ausiliaria e si occupa della gestione unitaria di AISE e AISI. Oltre a controllarne l'operato (la conformità alle leggi, ai regolamenti, alle direttive del Presidente) ne verifica i risultati[884] e raccoglie analisi e rapporti che provengono tanto dalle Agenzie quanto dalle forze armate e di polizia.[885] Così facendo, coordina l'intera attività di informazione per la sicurezza.[886] Con la creazione del DIS, il legislatore ha voluto creare *in primis* una struttura autorevole, capace di eliminare le sovrapposizioni e le ridondanze di costi dell'ordinamento precedente.[887] Il Dipartimento è stato altresì descritto come una "virtuosa strettoia istituzionale": un organo permanente capace di veicolare le informazioni tra i vertici delle Agenzie ed il decisore politico (i.e. il Presidente).[888]

---

[881] *Ibidem*, Art. 1(1); la riforma non fa che affermare e potenziare un ruolo che il Presidente rivestiva già nella legislazione previgente, vd. MASSERA A., MOSCA C., *I servizi d'informazione*, in Cassese (a cura di), Trattato di diritto amministrativo, diritto amministrativo speciale, Milano, 2000, p. 357: "[il Presidente del Consiglio è un] crocevia istituzionale dal quale si diramano e al quale fanno capo tutte le linee che collegano il sottosistema amministrativo costituito dagli organismi di informazione con le altre componenti del quadro istituzionale"; *cfr.* MOSCA C., *op. cit.* 41.
[882] MOSCA C., *op. cit.* 48.
[883] L. 124/2007, Art. 3; GIUPPONI T. F., *op. cit.* 14-15.
[884] MOSCA C., *op. cit.* 111: la verifica dei risultati non è agevole data la difficoltà di operare, in un contesto così particolare, una valutazione costi-benefici. Il DIS tenta piuttosto di trovare un "nesso convincente" tra investimenti nella ricerca informativa e i loro esiti.
[885] *Cfr.* MOSCA C., *op. cit.* 103.
[886] L. 124/2007, Art. 4.
[887] MOSCA C., *op. cit.* 104.
[888] *Ibidem*, 108.

L'AISE è l'Agenzia informazioni e sicurezza esterna.[889] A questa è affidato il compito di "ricercare ed elaborare nei settori di competenza tutte le informazioni utili alla difesa dell'indipendenza, dell'integrità e della sicurezza della Repubblica, anche in attuazione di accordi internazionali, dalle minacce provenienti dall'estero".[890] Si tratta di competenze vaste, che vanno ben oltre quelle del suo ideale predecessore (il SISMi) e si estendono potenzialmente a qualunque fenomeno, purché la provenienza territoriale sia esterna.[891] L'Agenzia possiede inoltre competenze esclusive nel campo della controproliferazione e del controspionaggio,[892] sempre a condizione che siano svolti al di fuori del territorio della Repubblica.

L'AISI è l'Agenzia informazioni e sicurezza interna.[893] Ha compiti analoghi a quelli dell'AISE, ma contenuti esclusivamente entro i confini della nazione. Ne garantisce la sicurezza interna e difende "le istituzioni democratiche poste dalla Costituzione a suo fondamento da ogni minaccia, da ogni attività eversiva e da ogni forma di aggressione criminale o terroristica."[894] La separazione nelle attribuzioni delle due Agenzie è netta: l'una non può operare nel territorio assegnato all'altra, salvo istituire una *task force* che veda la collaborazione di entrambe. Ciò è reso possibile, ex Artt. 6(4) e 7(4) della l. 124/2007, nei soli casi in cui le attività delle Agenzie siano tra loro connesse.

Sebbene il DIS coordini AISE e AISI, queste rispondono direttamente al Presidente del Consiglio (che ne nomina direttamente i vertici)[895] o all'Autorità Delegata. Per questo motivo si è detto che nel SIS non può riscontrarsi una gerarchia di tipo piramidale, quanto piuttosto un intreccio di diverse competenze.

A latere si trovano altre due figure istituzionali: il CISR ed il Copasir. Il primo è il Comitato interministeriale per la sicurezza della Repubblica, che ha un ruolo di consulenza e proposta circa gli indirizzi generali della politica di

[889] L. 124/2007, Art. 6(1).
[890] *Ibidem*.
[891] MOSCA C., *op. cit.* 138.
[892] *Cfr. Ibidem*: il nuovo riparto delle competenze è sostanzialmente diverso da quello del SISMi, che e.g. conduceva attività di controspionaggio sia nel territorio che all'estero, seguendo un criterio funzionale.
[893] L. 124/2007, Art. 7(1).
[894] *Ibidem*; MOSCA C., *op. cit.* 142-143: si noti che le minacce consistenti in "ogni forma di aggressione militare o terroristica" non devono rispondere al requisito dell'eversività, che rimane una fattispecie disgiunta.
[895] L. 124/2007, Artt. 1(1)(e), 6(5), 7(5).

intelligence.[896] È presieduto dal Presidente del Consiglio e vede riuniti i Ministri degli affari esteri, dell'interno, della difesa, dell'economia e delle finanze e dello sviluppo economico (con la partecipazione dell'Autorità Delegata, ove presente).[897] Il direttore del DIS svolge tra l'altro la funzione di sottosegretario del CISR,[898] mentre i direttori di AISE e AISI possono essere chiamati a partecipare alle singole sedute, previa loro richiesta e senza diritto di voto.[899] Visto il ruolo del tutto marginale rivestito dal precursore del Comitato (i.e. il CIIS, Comitato interministeriale per l'informazione e la sicurezza), il legislatore della riforma ha tentato di attribuire al nuovo organo funzioni più incisive.[900] I nuovi compiti di deliberazione circa la ripartizione delle risorse finanziarie tra DIS e Agenzie si muovono in questo senso.[901] Lo stesso si dica della possibilità, attribuita ai membri CISR, di essere auditi dal Copasir.[902] Infine, è disposto che il Comitato sia sentito dal Presidente del Consiglio prima dell'emanazione di "ogni disposizione necessaria per l'organizzazione e il funzionamento del Sistema di informazione per la sicurezza della Repubblica".[903] È stato osservato (*in primis* nel dibattito parlamentare post-riforma) che il nuovo Comitato non è stato strutturato come una "versione ristretta del Consiglio dei ministri", giacché la tendenza è piuttosto quella di accentrare il momento decisionale unicamente nel Presidente.[904] Ciononostante è stato auspicato[905] che il CISR si imponga sempre come interlocutore attivo nell'elaborazione delle politiche di sicurezza nazionale, rifiutando di essere relegato a mera sede di ratificazione delle decisioni del Presidente del Consiglio.

---

[896] GIUPPONI T. F., *op. cit.* 13; l. 124/2007, Art. 5(1); MOSCA C., *op. cit.* 52: "l'indirizzo monocratico [del Presidente del Consiglio] è solo parzialmente e in modo sostanzialmente minimale attenuato dall'ampiamento delle interlocuzioni riservate al CISR, in termini di formulazioni di pareri, considerato che tale alto organismo permane […] nella preminente posizione di organo di consulenza e proposta, cui si aggiungono limitati compiti di deliberazione sugli indirizzi e sulle finalità generali della politica dell'informazione per la sicurezza e taluni altri compiti propri".
[897] L. 124/2007, Art. 5(3).
[898] *Ibidem*, Art. 5(4).
[899] *Ibidem*, Art. 5(5).
[900] MOSCA C., *op. cit.* 75-76.
[901] L. 124/2007, Art. 5(2); MOSCA C., *op. cit.* 75.
[902] MOSCA C., *op. cit.*
[903] L. 124/2007, Art.1(3); MOSCA C., *op. cit.*
[904] MOSCA C., *op. cit.* 76.
[905] MOSCA C., *op. cit.* 77.

Il Copasir (Comitato parlamentare per la sicurezza della Repubblica) è il punto di contatto tra Governo e Parlamento in materia di *intelligence*.[906] Esso "verifica, in modo sistematico e continuativo, che l'attività del Sistema di informazione per la sicurezza si svolga nel rispetto della Costituzione, delle leggi, nell'esclusivo interesse per la difesa della Repubblica e delle sue istituzioni".[907] È composto da cinque membri per ogni Camera, nominati dai rispettivi presidenti tenendo conto della proporzione intercorrente tra maggioranza e gruppi di opposizione.[908] Il Comitato riveste funzioni di controllo e consultive di tipo prettamente politico, essenziali per garantire la compatibilità del SIS con l'ordinamento democratico della Repubblica. Costituisce il *trait d'union* tra potere esecutivo e legislativo che manca (*rectius* è presente ma privo di poteri effettivi)[909] negli Stati Uniti, rendendo estremamente ostico nel corso degli anni un reale sindacato sull'attività dei servizi segreti federali. Al contrario, i poteri conoscitivi del Copasir sono piuttosto incisivi: i.a. audizioni periodiche dei vertici del SIS, richieste di copie di atti anche in deroga all'Art. 329 cpp,[910] accessi e sopralluoghi, controllo della documentazione di spesa. Nello svolgimento dei controlli più delicati, i.e. quelli inerenti alla corrispondenza tra i comportamenti tenuti dai funzionari dei servizi segreti ed i loro compiti istituzionali previsti *ex lege*, non può essere opposta nessuna esigenza di riservatezza se la richiesta di informazioni è stata deliberata all'unanimità.[911] Fatto salvo questo particolare caso, si deve ritenere che il segreto di Stato sia comunque opponibile, riducendo notevolmente i poteri del Comitato.[912]

---

[906] BIANCO E., *op. cit.* 6; *cfr*. l. 124/2007, Art. 30; MOSCA C., *op. cit.* 368-371.
[907] L. 124/2007, Art. 30(2).
[908] L. 124/2007, Art. 30. Maggioranza e opposizione devono comunque essere rappresentate in modo paritario. Il presidente del Copasir è sempre un membro dell'opposizione, vd. l. 124/2007, Art. 30(3).
[909] *Cfr*. Capitolo II *supra*.
[910] Salva la possibilità di opporre una specifica "esigenza di riservatezza" volta a preservare la sicurezza della Repubblica, i rapporti con Stati esteri, lo svolgimento di operazioni in corso o l'incolumità di informatori, collaboratori e membri dei servizi di *intelligence*. Il Presidente del Consiglio può sempre pronunciarsi contro la sussistenza di tale esigenza. Vd. l. 124/2007, Art. 31(7)(8)(9).
[911] L. 124/2007, Art. 31; GIUPPONI T. F., *op. cit.* 28; MOSCA C., *op. cit.* 378-379: inoltre al Copasir non sono opponibili il segreto d'ufficio, il segreto bancario e il segreto professionale (eccezion fatta per il segreto tra difensore e parte processuale).
[912] MOSCA C., *op. cit.* 379.

Il Copasir svolge anche incarichi di tipo consultivo. Il più importante fra questi è la stesura di una relazione annuale destinata al Parlamento "per riferire sull'attività svolta e per formulare proposte e segnalazioni su questioni di propria competenza". [913] Il Presidente del Consiglio, parallelamente, è tenuto a comunicare su base semestrale gli esiti delle attività del SIS, l'analisi della situazione e dei pericoli per la sicurezza, l'organizzazione ed il funzionamento dei servizi. [914] In particolar modo, l'Art. 33(4) prevede che il premier informi il Comitato circa le operazioni, compiute dalle Agenzie, che sono prevedute dalla legge come reato. [915]

Si tratta delle cd. "garanzie funzionali", [916] che forniscono agli agenti operativi una vera e propria causa di giustificazione speciale. Entro certi limiti e con le dovute precauzioni, [917] è loro consentito di compiere attività che sarebbero normalmente giudicate come criminose. La condizione primaria è ovviamente che tali contegni risultino indispensabili per le finalità istituzionali dei Servizi. [918] Si impone altresì che le condotte in questione siano state previamente autorizzate, volta per vota e nel rispetto rigoroso dei limiti imposti dalla legge. [919] Il controllo su queste condotte (autorizzate ma pur sempre *contra legem*) spetta al Copasir soltanto nel merito, *ergo* sul piano strettamente politico. Il Controllo di legittimità è assegnato invece alla Corte Costituzionale, quando adita dall'autorità giudiziaria procedente. [920]

---

[913] GIUPPONI T. F., *op. cit.*; l. 124/2007, Art. 35. Durante l'anno è sempre possibile trasmettere informative o relazioni urgenti.
[914] L. 124/2007, Art. 35; MOSCA C., *op. cit.* 373-374.
[915] MOSCA C., *op. cit.* 375: il presidente è tenuto solo a comunicare solo l'effettivo svolgimento di tali attività, non anche la mera autorizzazione cui non sia stata data esecuzione.
[916] *Cfr.* l. 124/2007, Art. 17, 18, 24, 25.
[917] Innanzitutto è necessaria la previa autorizzazione governativa, vd. *Ibidem*, Art. 18. Alcuni reati rimangono comunque preclusi, vd. *Ibidem*, Art. 17(2): "delitti diretti a mettere in pericolo o a ledere la vita, l'integrità fisica, la personalità individuale, la libertà personale, la libertà morale, la salute o l'incolumità di una o più persone". *Cfr*. anche *Ibidem*, Art. 17(3).
[918] MOSCA C., *op. cit.* 243.
[919] *Cfr.* MOSCA C., *op. cit.* 244-245; ex Art. 17(7) l. 124/2007 le garanzie funzionali possono estendersi anche ai non appartenenti ai servizi nei casi di concorso. Tuttavia, i requisiti delle "eccezionali necessità" e delle "particolari condizioni di fatto" rendono la norma di difficile applicazione.
[920] Il normale *iter* presuppone che il giudice, una volta opposta la causa di giustificazione speciale, pronunci sentenza di non luogo a procedere o di assoluzione. Qualora ritenga che le proprie attribuzioni costituzionali siano state menomate dall'uso illegittimo delle garanzie funzionali,

2.2. Il segreto di Stato

L'ultima novità di rilievo, introdotta nel nostro ordinamento dalla legge del 2007, riguarda la disciplina del segreto di Stato. Nella giurisprudenza della Corte Costituzionale, tale controverso istituto trova la sua legittimazione:

> nell'esigenza di salvaguardare supremi interessi riferibili allo Stato-comunità, ponendosi quale «strumento necessario per raggiungere il fine della sicurezza», esterna e interna, «dello Stato e per garantirne l'esistenza, l'integrità, nonché l'assetto democratico»: valori che trovano espressione in un complesso di norme costituzionali, e particolarmente in quelle degli artt. 1, 5 e 52 Cost. (sentenza n. 110 del 1998; in prospettiva analoga, sentenze n. 106 del 2009, n. 86 del 1977 e n. 82 del 1976).[921]

Si tratta di un orientamento consolidato negli anni, precedente alla riforma e immutato alla luce del quadro normativo odierno.[922]

Ex Art. 39 l. 124/2007, sono coperti dal segreto "gli atti, i documenti, le notizie, le attività e ogni altra cosa la cui diffusione sia idonea a recare danno all'integrità della Repubblica, anche in relazione ad accordi internazionali, alla difesa delle istituzioni poste dalla Costituzione a suo fondamento, all'indipendenza dello Stato rispetto agli altri Stati e alle relazioni con essi, alla preparazione e alla difesa militare dello Stato".[923] Rispetto alla precedente disciplina, dettata ex Art. 12 l. 801/1977, traspare la volontà di specificare con

---

solleverà conflitto di fronte al giudice delle leggi. Vd. GIUPPONI T. F., *op. cit.* 30; l. 124/2007, Art. 19(8).

[921] Corte Costituzionale, Sentenza n 40/2012 §5.

[922] C*fr.* Corte Costituzionale, Sentenza n 106/2009: "[v]a affermata la perdurante attualità dei principi tradizionalmente enunciati dalla giurisprudenza costituzionale in materia di segreto di Stato, pur a seguito della introduzione delle nuove disposizioni di cui alla legge 3 agosto 2007, n. 124. La disciplina del segreto involge il supremo interesse della sicurezza dello Stato nella sua personalità internazionale, cioè l'interesse dello Stato-comunità alla propria integrità territoriale e alla propria indipendenza, interesse che trova espressione nell'art. 52 Cost. in relazione agli artt. 1 e 5 Cost. Il segreto in oggetto pone necessariamente un problema di interferenza con altri principi costituzionali, inclusi quelli che reggono la funzione giurisdizionale: in quest'ambito, l'apposizione del segreto da parte del Presidente del Consiglio dei ministri non può impedire che il pubblico ministero indaghi sui fatti di reato, ma può inibire all'autorità giudiziaria di acquisire ed utilizzare gli elementi di conoscenza coperti dal segreto. In materia, il Presidente del Consiglio gode di un ampio potere discrezionale, sul cui esercizio è escluso qualsiasi sindacato giurisdizionale, poiché il giudizio sui mezzi idonei a garantire la sicurezza dello Stato ha natura politica."

[923] L. 124/2007, Art. 39(1).

maggior metodicità l'ambito di applicazione oggettiva della norma.[924] Ancora, gode di maggior chiarezza la classificazione secondo quattro livelli di tutela: segretissimo, segreto, riservatissimo e riservato.[925] Tali classi sono assegnate sulla base di criteri, dettati con apposito DPCM,[926] proporzionali al danno che potrebbe scaturire da un'eventuale pubblicazione delle informazioni secretate.[927]

La vera peculiarità della nuova legge risiede nella "temporizzazione"[928] del segreto di Stato. Decorsi quindici anni dalla sua apposizione (od opposizione ex Art. 202 cpp), "chiunque vi abbia interesse" può inoltrare una richiesta al Presidente del Consiglio al fine di ottenere l'accesso alle informazioni classificate.[929] La richiesta è accolta entro 30 giorni salvo che il Presidente non ritenga di dover prorogare il vincolo di segretezza. Comunque, la durata complessiva del segreto non può superare i 30 anni. In qualunque momento precedente, il vincolo può essere fatto decadere se risultano cessate le esigenze originarie di tutela.[930]

La corretta applicazione delle politiche in materia di segreto di Stato è affidata al DIS che, attraverso un ufficio dedicato (l'UCSe i.e. "Ufficio Centrale per la Segretezza"),[931] rilascia e revoca i nullaosta di sicurezza (NOS) seguendo le

[924] L'Art. 12, 1° comma, l. 801/1977 recitava genericamente "atti, documenti, notizie, attività e ogni altra cosa"; GIUPPONI T. F., *op. cit.* 33: in risposta al conflitto di attribuzione tra Presidente del Consiglio e magistratura di Tempio Pausania nel caso "Villa La Certosa", il legislatore ha aggiunto espressamente il riferimento ai luoghi. Vd. Corte Costituzionale, Ordinanza n 404/2005; *cfr.* MOSCA C., *op. cit.* 538-540: l'autore critica la novella per un approccio definitorio ancora non perfettamente marcato, ma "ibrido". Molti possibili casi di apposizione del segreto non sono stati ancora indicati. Nel silenzio del legislatore, lo sforzo ermeneutico dell'interprete può portare di volta in volta a esiti differenti, sfavorendo l'interazione tra poteri dello Stato.

[925] MOSCA C., *op. cit.* 751-753: l'attribuzione della classifica di segretezza è un provvedimento amministrativo appartenente alla *species* degli ordini. Ex. Art. 42, comma 2, l. 124/2007 i criteri di scelta delle classifiche di segretezza si basano su criteri "ordinariamente seguiti nelle relazioni internazionali". Si tratta di fonti miscellanee, vd. i.a. Decisione del Consiglio 2001/264/CE del 19 Marzo 2001; Decisione della Commissione 2001/844/CE; NATO Document C-M (2002) 49; Accordo di Sicurezza dell'Unione Europea Occidentale del 28 Marzo 1995.

[926] Vd. DPCM 8 Aprile 2008, in particolare Art. 5.

[927] Si noti che, nella pratica, i primi tre livelli di classificazione (segretissimo, segreto, riservatissimo) si sovrappongono spesso, essendo di difficile distinzione. Le informazioni "riservate" sono individuate in negativo rispetto alle prime tre classi e sono sottoposte ad un regime di divulgazione meno rigido. *Cfr*. *Ibidem*; GIUPPONI T. F., *op. cit.* 32-37.

[928] BIANCO E., *op. cit.* 5.

[929] L. 124/2007, Art. 39(7).

[930] GIUPPONI T. F., *op. cit.* 35; l. 124/2007, Art. 39(8)(9).

[931] L. 124/2007, Art. 9(1).

disposizioni del Presidente del Consiglio.[932] Il controllo *ex post* compete invece, esattamente come accade per le garanzie funzionali, al Copasir (giudizio di merito) e alla Corte Costituzionale (legittimità). Il giudice delle leggi ha di fatto l'ultima parola in materia di segreto di Stato, che non gli può essere opposto in nessun caso.[933] Perciò, se nel corso di un processo penale viene opposto il segreto così da non ottemperare ad una richiesta di esibizione o acquisizione documentale, può essere sollevato conflitto di attribuzione. In questo modo il legislatore ha cercato di bilanciare due valori giuridici di pari dignità: la sicurezza della Repubblica e l'obbligatorietà dell'azione penale connessa all'esercizio indipendente della funzione giudiziaria.[934]

Le difficoltà del cd. "Giudice del segreto"[935] in questo campo sono notevoli. Le complicazioni maggiori sorgono quando si tenta di tracciare la linea di demarcazione tra giudizio di merito (che è precluso al potere giudiziario) e di legittimità. Nel già citato caso *Abu Omar*[936] è stato confermato che:

> è escluso […] qualsiasi sindacato sull'*an*, ma anche sul *quomodo* del potere di segretazione, atteso che il giudizio sui mezzi idonei e necessari per garantire la sicurezza dello Stato ha natura squisitamente politica e, quindi, mentre è connaturale agli organi ed alle autorità politiche preposte alla sua tutela, certamente non è consono alla attività del giudice.[937]

I poteri del giudice delle leggi di conseguenza sono assai limitati, poiché il sindacato della Corte viene confinato ad un mero controllo di conformità alle procedure prescritte *ex lege*. Neppure vengono esaminate le motivazioni degli atti, o la loro proporzionalità rispetto allo scopo perseguito, dato che "il giudizio sui mezzi ritenuti necessari o soltanto utili a garantire la sicurezza dello Stato spetta al Presidente del Consiglio dei ministri sotto il controllo del Parlamento".[938] Un

---

[932] *Ibidem*, Art. 9(2)(c); MOSCA C., *op. cit.* 7555-756: "Il NOS è rilasciato all'esito di un procedimento diretto ad escludere che le notizie, documenti, cose, classificate siano conosciute da soggetti che non diano sufficiente garanzia di fedeltà alle istituzioni della Repubblica, alla Costituzione e ai suoi valori, nonché di rispetto del segreto".
[933] GIUPPONI T. F., *op. cit.* 44; l. 124/2007, Art. 40(7)(8).
[934] GIUPPONI T. F., *op. cit.*
[935] Così è stata definita la Corte Costituzionale i.a. da *cfr.* BARILE P., *Democrazia e segreto*, in Quad. Cost., 1987, 40.
[936] Corte Costituzionale, Sentenza n 106/2009.
[937] *Cfr.* anche Corte Costituzionale, Sentenza n 86/1977.
[938] Corte Costituzionale, Sentenza n 106/2009; GIUPPONI T. F., *op. cit.* 47.

simile approccio non è stato esente da critiche. Parte della dottrina,[939] invocando l'Art. 202 comma 7 c.p.p.,[940] ha sostenuto che la Corte ha il potere-dovere di effettuare un controllo sull'*an* e sul *quomodo* al fine di verificare che il vincolo di segretezza sia stato posto legittimamente.[941] Soprattutto, nel controllo di proporzionalità non andrebbe ravvisato un atto politico *tout court*, quanto un "sindacato sul corretto esercizio della discrezionalità alla luce della Costituzione".[942]

In tempi recentissimi la Corte Costituzionale è tornata a trattare la questione.[943] Il Presidente del Consiglio, sempre nel contesto dell'annosa vicenda *Abu Omar*, ha proposto due ricorsi per conflitto di attribuzione.[944] L'Avvocatura generale dello Stato impugnava, in prima battuta, la sentenza n. 46340/2012 della Cassazione penale, la quale annullava con rinvio la precedente sentenza della Corte d'Appello di Milano (n. 3688/2010). Questa a sua volta aveva confermato la declaratoria di improcedibilità ex Art. 202 c.p.p.[945] disposta già in primo grado. Inoltre, il ricorrente contestava l'annullamento di due ordinanze (del 22 e 26 Ottobre 2010) che disponevano l'inutilizzabilità delle dichiarazioni rese da quattro degli indagati nel corso di interrogatori svolti durante le indagini preliminari. La Cassazione oltretutto, puntualizzava l'Avvocato Generale, si sarebbe arbitrariamente ingerita nelle attribuzioni del Presidente del Consiglio, limitando la portata oggettiva del segreto di Stato apposto da quest'ultimo. Infatti, pur affermando che il segreto copriva "documenti e notizie riguardanti i rapporti tra Servizi italiani e stranieri e sugli *interna corporis*, anche se relativi alla vicenda

[939] Vd. i.a. SALVI G., *La Corte Costituzionale e il segreto di Stato*, in Cass. Pen., 2009, 3758ss.; BONZANO C., *Il segreto di Stato nel processo penale*, Padova, 2010, 281; ORLANDI R., *Segreto di Stato e limiti alla sua opponibilità*, in Giur. Cost., 2010, 5227ss.

[940] "Quando è sollevato conflitto di attribuzione nei confronti del Presidente del Consiglio dei Ministri, qualora il conflitto sia risolto nel senso dell'insussistenza del segreto di Stato, il Presidente del Consiglio dei Ministri non può più opporlo con riferimento al medesimo oggetto. Qualora il conflitto sia risolto nel senso della sussistenza del segreto di Stato, l'autorità giudiziaria non può né acquisire né utilizzare, direttamente o indirettamente, atti o documenti sui quali è stato opposto il segreto di Stato."

[941] *Cfr.* ARCONZO G., *Il segreto di Stato nella giurisprudenza della Corte Costituzionale e della Corte europea dei diritti dell'uomo*, in AIC rivista telematica, 2012, 16.

[942] ANZON A., *Il segreto di Stato, ancora una volta tra stato e costituzione*, in Giur. Cost., 1976, 1031; ARCONZO G., *op. cit.*

[943] Corte Costituzionale, Sentenza n 24/2014.

[944] Notificati, rispettivamente, il 24 Aprile ed il 4 Febbraio 2013.

[945] Vd. Art. 202 comma 3 c.p.p.: "qualora il segreto sia confermato e per la definizione del processo risulti essenziale la conoscenza di quanto coperto dal segreto di Stato, il giudice dichiara non doversi procedere per l'esistenza del segreto di Stato."

delle *renditions* e del sequestro di Abu Omar", la Cassazione circoscriveva detto segreto alle sole operazioni svolte di concerto da SISMi e CIA. A fondamento di un simile approccio stava la nota dell'11 Novembre 2005,[946] con cui il Governo dichiarava la propria estraneità (nonché quella dei servizi segreti italiani) alla vicenda *Abu Omar*. Assumendo la veridicità del contenuto della nota, gli imputati avrebbero agito al di fuori delle funzioni ufficiali e non sarebbero stati perciò "schermati" dal segreto.[947]

Il secondo ricorso riguardava consequenzialmente il giudizio rescissorio i.e. la sentenza di rinvio pronunciata dalla Corte d'Appello di Milano (n. 985/2013) all'esito della quale venivano condannati i vertici del SISMI allora in carica.[948] Soprattutto, si contestava che la Corte milanese, uniformandosi al dispositivo del giudice di legittimità, avesse omesso l'interpello del Presidente per la conferma del segreto di Stato opposto dagli imputati sul contenuto dei verbali degli interrogatori summenzionati. Questi elementi, al contrario, erano stati utilizzati e posti a fondamento della sentenza di condanna. In questo modo la Corte avrebbe violato il principio di leale collaborazione tra poteri dello Stato.[949]

Il giudice delle leggi, richiamando la precedente giurisprudenza,[950] a sostegno delle doglianze della difesa erariale rammentava che:

> la disciplina del segreto involge il supremo interesse della sicurezza dello Stato-comunità alla propria integrità e alla propria indipendenza, interesse che trova espressione nell'Art. 52 della Costituzione in relazione agli artt. 1 e 5 della medesima Carta. D'altra parte, tenuto conto della ampiezza e della intensità del vincolo che consegue alla apposizione e conferma di tale particolare figura di segreto, scaturiscono necessariamente dal relativo regime profili di interferenza con altri principi costituzionali, inclusi quelli che reggono la funzione giurisdizionale.[951]

Per ciò solo non può essere impedito ovviamente al PM di indagare sul fatto storico integrante una notizia di reato, ma si può inibire all'autorità giudiziaria di

[946] Nota Prot. USG/2-SP/1318/50/347 dell'11 Novembre 2005.
[947] Corte di Cassazione, Cass. pen., Sez. V, 19 Settembre 2012, n.46340, pp. 123-124.
[948] Si tratta di Nicolò Pollari, Raffaele Di Troia, Giuseppe Ciorra, Marco Mancini, Luciano Di Gregori.
[949] Corte Costituzionale, Sentenza n 24/2014.
[950] Corte Costituzionale, Sentenza n 106/2009; Corte Costituzionale, Sentenza n 86/1977.
[951] Corte Costituzionale, Sentenza n 24/2014, §5.

acquisire ed utilizzare mezzi di prova secretati. Il principio vale, *mutatis mutandis*, qualora sia preclusa una fonte di prova essenziale e si debba perciò pronunciare sentenza di non luogo a procedere.[952] L'oggetto del segreto è circoscritto all'interno di un "perimetro tracciato dal Presidente del Consiglio dei Ministri" nell'esercizio di un potere di natura "squisitamente politica". La Corte Costituzionale, sottraendo le condotte "extrafunzionali" degli agenti del SISMi da tale perimetro, aveva modificato nella portata e nel contenuto l'oggetto del segreto. La tesi secondo cui gli imputati avrebbero agito a titolo personale, per di più, era intrinsecamente contraddetta dall'applicazione dell'aggravante ex Art. 605, secondo comma, n.2 c.p. ("[l]a pena è della reclusione da uno a dieci anni, se il fatto è commesso: […] 2) da un pubblico ufficiale, con abuso dei poteri inerenti alle sue funzioni").[953]

La Corte Costituzionale proseguiva la sua disamina con un'argomentazione quantomeno ambigua. Prendendo le mosse dall'Art. 18(6) l. 124/2007,[954] viene asserito che nel caso in cui la condotta posta in essere dagli agenti del SISMi indagati non fosse stata espressamente autorizzata dal Presidente del Consiglio, questi avrebbe informato l'autorità giudiziaria senza ritardo. Al contrario, la "ribadita e confermata" sussistenza del segreto e il promovimento dei conflitti di attribuzione proverebbe che le condotte in esame non potevano essere state compiute a titolo personale.[955] In tale prospettiva, concludeva la Corte, "pare arduo negare che la copertura del segreto […] si proietti su tutti i fatti, notizie e documenti concernenti le eventuali direttive operative, gli *interna corporis* di carattere organizzativo e operativo, nonché i rapporti con i Servizi stranieri, anche se riguardanti le *renditions* ed il sequestro di Abu Omar. Ciò, ovviamente, a condizione che gli atti e i comportamenti degli agenti siano oggettivamente orientati alla tutela della sicurezza dello Stato".[956] Un simile ragionamento, per quanto coerente, potrebbe essere fallace nelle premesse. La Corte sembra essersi preoccupata unicamente dell'evenienza in cui sia il potere giudiziario a menomare

[952] *Ibidem*.
[953] *Ibidem*, §6.
[954] "Nei casi in cui la condotta prevista dalla legge come reato sia stata posta in essere in assenza ovvero oltre i limiti delle autorizzazioni previste dal presente articolo, il Presidente del Consiglio dei ministri adotta le necessarie misure e informa l'autorità giudiziaria senza ritardo".
[955] Corte Costituzionale, Sentenza n 24/2014, §7.
[956] *Ibidem*.

arbitrariamente le prerogative dell'esecutivo. D'altro canto, è ben possibile che accada l'opposto. In particolare, è stato dato per scontato che, configurandosi una situazione ex Art. 18(6) l. 124/2007, il Presidente del Consiglio adotti sempre le misure necessarie impostegli dalla legge. *Quid* se fosse stato invece il governo ad agire arbitrariamente, con l'intento di garantire ai propri agenti l'impunità per un crimine da essi compiuto? Senza voler scendere nel merito della questione, la divergenza fra dichiarazioni precedenti (i.e. la nota dell'11 Novembre 2005) e comportamenti successivi (i conflitti di attribuzione sollevati) suggerisce se non altro la possibilità di un comportamento illegittimo, indipendente dalla sicurezza dello Stato. Possibilità sulla quale la Corte, essendo l'unico organo dello Stato al quale non può opporsi il segreto, avrebbe potuto porre una maggiore attenzione.

2.3. Considerazioni

Alla luce di quanto esposto finora, il SIS è un apparato fatto di limiti e contro-limiti che consente, in teoria, di gestire l'attività di *intelligence* nel rispetto dei principi fondamentali della nostra costituzione. Nella pratica non è esente da difetti. La partecipazione ed il controllo da parte di Copasir e Corte Costituzionale sono strumenti validissimi per garantire una fisiologica separazione dei poteri, ma si rendono necessari degli accorgimenti.

In primo luogo in dottrina[957] è stata criticata aspramente l'assenza, nel comparto *intelligence*, del Presidente della Repubblica (in veste di comandante supremo delle Forze Armate)[958] e del Consiglio supremo di difesa. D'altro canto è stato giustamente osservato che il Capo di Stato può e deve avere un ruolo attivo di garante costituzionale in relazione alle attività di *intelligence* più sensibili, pur non partecipando direttamente all'indirizzo politico del SIS.[959]

Una seconda criticità risiede nella relativa debolezza del Copasir. Il Comitato, infatti, svolge solo un'attività di controllo *ex post*. Questo anche nel delicato ambito delle garanzie funzionali.[960] Inoltre, qualora ravvisi una violazione della normativa vigente da parte dei servizi segreti, non è tenuto

[957] BONETTI P., *Aspetti costituzionali del nuovo sistema di informazione per la sicurezza della Repubblica*, in Dir. soc., 2008, 251 ss.
[958] *Cfr.* Art. 87 Cost.
[959] GIUPPONI T. F., *op. cit.* 13.
[960] L. 124/2007, Art. 34.

espressamente a darne comunicazione all'autorità giudiziaria, bensì solo al Presidente del Consiglio e ai Presidenti delle Camere. Ciò considerato, è più che benvenuto il protocollo di intenti siglato tra DIS e Garante della *privacy*, che consente quantomeno un controllo indipendente *ex ante* in materia di trattamento dei dati personali e intercettazioni.

Infine, come già anticipato, la Corte Costituzionale non ha un approccio sufficientemente pragmatico. Tanto in materia di garanzie funzionali che di segreto è "relegata" al sindacato di legittimità. Il rischio di invadere la sfera politica del Copasir, in effetti, è alto e la Corte è sempre stata estremamente cauta nella giurisprudenza pregressa. Tuttavia, limitarsi ad una verifica esterna dei requisiti formali degli atti posti in essere dalle Agenzie significa svilire completamente l'utilità del conflitto di attribuzione. L'eventualità che anche i nostri servizi segreti abbiano preso parte attivamente al *datagate* richiede una risposta più audace. Si auspica che, nei futuri casi di conflitto, il giudice delle leggi si schieri con maggior decisione dalla parte delle libertà civili. Il controllo di legittimità deve essere esteso alla necessità e alla proporzionalità (dunque alla non arbitrarietà) delle condotte del SIS, siano esse reati compiuti sotto l'egida delle garanzie funzionali o apposizioni del segreto di Stato.

CONCLUSIONI

Terminata la disamina degli aspetti giuridici più rilevanti in merito all'*intelligence gathering*, si direbbe possibile rispondere a buona parte alle domande sorte nelle fasi iniziali della trattazione.

Sul versante del diritto internazionale in tempo di pace, come premesso, la materia si è rivelata alquanto composita. Da una parte l'eterogeneità delle tematiche (diritto diplomatico, del mare, tutela della *privacy* e dei dati personali) ha offerto risposte diverse a seconda delle situazioni. Dall'altra, gli avvenimenti recenti (tra cui il *datagate* spicca per il proprio clamore, senza essere per ciò solo l'unico esempio macroscopico) stanno aprendo la strada ad una nuova visione politico-giuridica dell'intelligence e dunque ad una più definita *opinio juris*. Nel secolo scorso l'*intelligence* si traduceva essenzialmente in spionaggio e controspionaggio tra blocchi opposti. Un tema tanto delicato, innestandosi nelle meccaniche proprie della Guerra Fredda, ha finito con l'essere inglobato nella logica del deterrente. Le conseguenze sono state diffusamente illustrate: gli attori internazionali hanno prediletto sistematicamente soluzioni del tipo *tit-for-tat* senza mai concretamente affrontare la questione, che inevitabilmente ha occupato la *grey area* del silenzio normativo. Eppure, nel ricco arsenale delle convenzioni internazionali, erano già presenti tutti gli strumenti necessari al giurista. Fintantoché le tecnologie esistenti non hanno consentito l'impiego estensivo dei mezzi di SIGINT, si poteva pacificamente asserire che nulla di illecito era ravvisabile nell'*intelligence collection* per sé considerata. Diversamente, lo spionaggio era ed è tuttora illecito *de facto*: porre in essere simili azioni clandestine implica necessariamente la violazione della sovranità territoriale altrui e dei principi di *friendly neighborood*. Se almeno parte delle controversie in materia (e come si è visto non sono state infrequenti) fossero state sottoposte ad

un organo giurisdizionale internazionale, ovviamente, sarebbe stato possibile definirne con maggior chiarezza i limiti.

Lo sviluppo tecnologico della *digital age* ha reso possibili nuove modalità di raccolta delle informazioni da remoto, inaugurando una nuova generazione di *intelligence*. Se oggi lo spionaggio *stricto sensu* è relegato a pochi casi isolati, Echelon, PRISM o XKeyscore sono divenuti la realtà quotidiana con cui si devono misurare i legislatori nazionali. La *opinio juris* nascente nei confronti della *bulk data collection* è evidente e coesa nel condannare tale pratica. A livello globale si nota come standard simili a quelli impostati dalla Direttiva 46/95/CE siano presi come punto di riferimento anche tra i paesi extracomunitari. Si è trattato in larga parte di un processo inerziale, quasi inconscio, suffragato infine dalla Risoluzione A/RES/68/167. Questa prevede i.a. che l'Assemblea Generale torni ad affrontare il problema della *mass surveillance* nel corso della sessantanovesima sessione, che si sta riunendo a New York mentre vengono scritte queste righe. Alla luce delle osservazioni presentate dallo *special rapporteur* Frank La Rue, è ben probabile che nei prossimi giorni sia redatta una nuova risoluzione dichiarativa dei principi riconosciuti dalla maggioranza dei paesi democratici e dalla società civile.[961] Un'ottima cornice su cui impostare i lavori (richiamata anche dal suddetto *report*) è stata fornita nei mesi scorsi dalla *Electronic Frontier Foundation*.[962] Si tratta di un'organizzazione *non-profit* attiva nella tutela delle libertà civili, la quale ha elaborato una lista di tredici principi che gli Stati sono chiamati a seguire qualora pongano in essere attività di sorveglianza telematica.[963] Il pregio di questo novero è quello di raggruppare in un'unica sede le prescrizioni delle principali Convenzioni internazionali richiamate nelle pagine precedenti, che vengono raffinate e attualizzate:

- Legalità: qualunque limitazione dei diritti umani deve essere adottata in forza di un atto legislativo definito e pubblicamente accessibile;

[961] Vd. in proposito il discorso di apertura alla 27° sessione dello *Human Rights Council* tenutosi il 12 Settembre 2014: http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15022&LangID=E.
[962] https://www.eff.org/about.
[963] Vd. https://en.necessaryandproportionate.org/.

- Scopo legittimo: la sorveglianza telematica deve essere consentita solo alle autorità pubbliche indicate dalla legge, per il conseguimento di un fine predominante e necessario in una società democratica;
- Necessità: leggi, regolamenti, poteri e autorità di sorveglianza devono limitarsi a quanto strettamente necessario per il perseguimento del fine legittimo;
- Adeguatezza: le attività di sorveglianza telematica autorizzate dalla legge devono essere appropriate in ragione del fine legittimo previsto;
- Proporzionalità: la sorveglianza telematica è un atto profondamente intrusivo. La sensibilità delle informazioni che si stanno per acquisire e il danno alla *privacy* del soggetto interessato devono essere tenuti in considerazione. L'autorità giudiziaria competente deve preventivamente accertare l'elevata probabilità che sia stato commesso un crimine grave e che dei mezzi meno pervasivi sarebbero inutili. Solo le informazioni utili devono essere conservate e consultate dall'autorità preposta;
- Autorità competente: l'autorità giudiziaria competente in materia di sorveglianza telematica deve essere imparziale e indipendente, nettamente distinta dall'autorità preposta alla sorveglianza stessa;
- Giusto processo: qualunque procedimento lesivo dei diritti umani deve essere previsto *ex lege*. Chiunque ha diritto a essere audito pubblicamente di fronte a un organo giurisdizionale equo, imparziale e precostituito dalla legge;
- Notificazione: le persone interessate dalla sorveglianza telematica devono ricevere una notifica concernente l'autorizzazione a procedere con l'intercettazione, in un tempo ragionevole e tale da consentire l'impugnazione del provvedimento;
- Trasparenza: gli Stati devono essere trasparenti per ciò che attiene a leggi, regolamenti, poteri e autorità in materia di sorveglianza telematica. In particolare, devono essere chiari lo scopo, la natura e la portata delle normative vigenti. Gli Stati non devono interferire con i gestori di servizi che intendono rendere pubbliche le modalità attraverso le quali danno applicazione alla normativa in questione;

- Controllo pubblico: gli Stati devono istituire dei meccanismi pubblici di controllo per assicurare trasparenza e responsabilità nella sorveglianza telematica. Tali organi devono poter accedere alle informazioni classificate, accertare che lo Stato si stia attenendo alla legislazione esistente, valutare l'accuratezza delle informazioni che lo Stato pubblica in ottemperanza all'obbligo di trasparenza. Devono inoltre pubblicare rapporti periodici in merito all'attività di monitoraggio svolta e alle risultanze della stessa;
- Integrità delle comunicazioni e dei sistemi: gli Stati non possono obbligare i gestori di servizi di telecomunicazioni ad installare nei propri prodotti *software* o *hardware* alcun sistema di sorveglianza. Non deve in nessun caso essere demandata la conservazione *a priori* dei dati presenti nelle banche dati dei gestori. Gli utenti hanno il diritto di restare anonimi;
- Cooperazione internazionale: per i trasferimenti transnazionali di dati personali per esigenze di polizia, devono sempre essere assicurati gli standard più elevati garantiti da una delle due parti in materia di *privacy*. Deve sempre applicarsi il principio della doppia incriminazione. Non deve in nessun caso essere richiesta la trasmissione di dati personali transfrontaliera al fine di aggirare la normativa nazionale. Gli accordi bilaterali di assistenza legale reciproca devono sempre essere documentati e pubblicamente accessibili;
- Tutele contro accessi illegittimi e diritto ad un rimedio effettivo: la sorveglianza illegale da parte di attori privati e pubblici deve essere criminalizzata. Devono essere stabilite pene o sanzioni adeguate, tutela ai *whistleblowers* e risarcimenti effettivi per le vittime. Le informazioni ottenute illegalmente devono essere sempre inutilizzabili nel procedimento giudiziario. I dati ottenuti attraverso l'attività di sorveglianza legittima non possono essere conservati una volta servito il proprio scopo.

A livello regionale sarà necessario attendere un certo tempo prima di poter verificare quanto saranno incisive, in materia di *privacy*, le politiche dei due

principali attori del *datagate* (i.e. USA e UE). Per ciò che concerne l'Europa, è poco probabile che il nuovo RGPD sia adottato nel prossimo futuro: gli interventi di Peter Hustinx, Viviane Reding e Antonello Soro (vd. *supra*) tradiscono un certo grado di sfiducia in proposito. A bloccare l'ingranaggio legislativo europeo, è stato detto, sono soprattutto gli interessi di lobby. Nel mondo digitale in cui viviamo, chiunque può attestare che la moneta più ricercata è il dato personale. Colossi del calibro di Google, Microsoft e Facebook hanno ridotto considerevolmente l'offerta di *software* a pagamento, proponendo piuttosto una pletora di applicazioni gratuite il cui utilizzo è condizionale all'immissione delle proprie generalità. In un mercato così configurato, una maggior tutela dei dati personali comporta primariamente un danno economico ingente alle imprese cd. *over-the-top*. In America, nel frattempo, la situazione è ancora profondamente incerta. La ACLU sta contribuendo al moto riformista nei confronti del sistema di *intelligence* nazionale sostenendo diverse cause, in primis quella instaurata da Twitter alla fine del mese di Luglio 2014.[964] Gli avvocati del famoso *social network* si batteranno in aula nei prossimi mesi per rivendicare il diritto di informare i propri utenti circa quali e quanti dati sono stati forzosamente acquisiti dalla NSA. Le norme sulla segretezza imposte dal governo, nelle intenzioni dell'accusa, devono essere dichiarate incostituzionali. Contemporaneamente, il Senatore Patrick Leahy (presidente della *Senate Judiciary Committee*) ha introdotto il disegno di legge per una nuova versione dello *USA Freedom Act*.[965] Si tratta di un testo estremamente significativo, che persegue lo scopo di porre fine alla *bulk data collection* e di ridurre drasticamente le capacità di sorveglianza delle *Agencies* in forza dello USA PATRIOT Act §215 (vd. *supra*). I segni per una riforma del diritto nazionale statunitense, pertanto, esistono e sono capaci di apportare un cambiamento concreto. Solo in un secondo momento, quando il cd. *transatlantic divide* con l'UE sarà realmente assottigliato, si potrà sperare in una fruttuosa conclusione dei negoziati sullo *Umbrella Agreement*. Il passo successivo è quello di integrare il quadro esistente con un *Safe Harbor* debitamente riformato, capace di far sopravvivere le proprie tutele anche alla presenza di esigenze di sicurezza nazionale.

[964] https://blog.twitter.com/2014/taking-the-fight-for-transparency-to-court.
[965] https://www.aclu.org/blog/national-security/senate-jumps-race-rein-nsa-surveillance.

In Italia, la percezione del *datagate* è parziale. La causa principale è la limitata quantità di informazioni in merito all'estensione della *mass surveillance* nel nostro paese. In secondo luogo, si ha l'impressione che in patria persista una profonda ineducazione informatica, che impedisce la crescita di una consapevolezza sociale circa l'importanza dei dati personali e dell'io digitale. Su questi due versanti è stato encomiabile lo sforzo del Garante. Per quanto riguarda l'educazione digitale, è impossibile parlare di risultati nel breve periodo. Si può solo osservare che l'Autorità, capeggiata da Antonello Soro, sta promuovendo una vasta campagna di sensibilizzazione attraverso conferenze, comunicati stampa e rivolgendosi alle scuole.[966] Sul fronte *intelligence*, come è stato detto, il protocollo d'intenti siglato con il DIS non ha precedenti in Europa e offre un modello che tutte le amministrazioni degli Stati membri dovrebbero imitare. In effetti, sarebbe senz'altro positivo inserire nel nuovo progetto di Regolamento (che pure è afflitto dai problemi appena menzionati) una previsione di questo genere, prescrivente la collaborazione tra autorità garanti e servizi segreti nazionali. Per massimizzare la trasparenza dei nostri servizi, nei limiti della ragionevolezza e della tutela della sicurezza nazionale, si ribadisce che sarebbe auspicabile un cambiamento nell'impostazione seguita dalla giurisprudenza costituzionale. Non è chiaro, infatti, perché non dovrebbe essere operato un giudizio di proporzionalità anche nell'apposizione (od opposizione) del segreto di Stato, considerando l'enorme capacità lesiva che questo istituto ha sul potere giurisdizionale. Non è costituzionalmente accettabile che, coperto dal "sipario nero"[967] del segreto, il governo garantisca l'immunità assoluta ai propri agenti, anche qualora abbiano compiuto violazioni gravi dei diritti fondamentali.

Infine, alcune osservazioni sul diritto internazionale in tempo di guerra. Nell'epoca dei droni e degli attacchi informatici, si potrebbe pensare che le disposizioni riguardanti il trattamento delle spie siano relegate alla speculazione accademica. Di contro, in tempi recenti stiamo assistendo ad un progressivo disincanto nei confronti dei conflitti a distanza: non è realistico condurre le ostilità senza *boots on the ground*. Lo stesso vale per la raccolta di informazioni. È a questo punto che sorgono dubbi sull'opportunità della tradizionale disciplina

[966] Vd. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2893366.
[967] Corte di Cassazione, Cass. pen., Sez. V, 19 Settembre 2012, n.46340.

regolante lo status della spia catturata. Rispondendo all'impostazione tradizionale nel diritto dei conflitti armati, per cui i combattenti sono soggetti spendibili (nei limiti imposti dal principio di umanità), essi sono svestiti dei privilegi di cui godrebbero come prigionieri di guerra. Come evidenziato *supra*, si tratta di un deterrente che è indirizzato primariamente alla parte belligerante, per marginalizzare il ricorso ad una pratica tanto dannosa. Di contro, le conseguenze ricadono unicamente sulla spia: possibili trattamenti inumani o degradanti, ridotte garanzie di un giusto processo, alte probabilità di essere condannati alla pena capitale. Pertanto, in questa sede si augura un'applicazione quanto più rigida possibile dell'Art. 75 API, al fine di garantire sempre un grado minimo di tutela dei diritti fondamentali riconosciuti alla persona. Nel caso in cui la parte belligerante nemica minacci di ignorare o abbia violato le disposizioni in parola, lo Stato nazionale dell'agente è tenuto ad attivarsi per proteggerlo. Solo questa condotta è compatibile con la natura universale, indisponibile e indivisibile dei diritti umani.

BIBLIOGRAFIA

MANUALI E MONOGRAFIE

- BONZANO C., *Il segreto di Stato nel processo penale* (Padova, 2010).
- BORREA ODRÌA A., *Las garantìas constitucionales: habeas corpus y amparo* (Lima, Libros Peruanos, 1992).
- M BURN, *The Debatable Land: A study of The Motive of the Spies in Two Ages* (London, Hamilton, 1970).
- CIRILLO G. P., *Il Codice sulla protezione dei dati personali* (Giuffrè, Milano, 2004).
- CONFORTI B., *Diritto Internazionale* (Editoriale Scientifica, 10a edn, 2014).
- Council of Europe, *Handbook on European Data Protection Law* (Luxemburg, Publications Office of the European Union, 2014).
- E DENZA, *Diplomatic Law* (Oxford, 3rd edn, 2008).
- Y DINSTEIN, *The Conduct of Hostilities under the Law of International Armed Conflict* (Cambridge University Press, 2nd edn, 2010).
- M DIXON, *International Law* (Oxford, 6th edn, 2007).
- G E DO NASCIMENTO, *Diplomacy in International Law* (Kluwer Academic Publiscer, 1973).
- S EDWARDS, *Barbary General: the Life of William H Eaton* (Prentice-Hall, 1968).
- M FINCH & S FAFINSKI, *Legal Skills* (Oxford, 4th edn, 2013).
- GROZIO U., *Le Leggi della Guerra e della Pace III* (Oxford, 1925).
- D J HARRIS, *Cases and Materials on International Law* (Sweet and Maxwell, 6th edn, 2005).

- J M HENCKAERTS & L DOSWALD-BECK, *Customary International Humanitarian Law Volume I: Rules* (Cambridge, 2009).
- J M HENCKAERTS & L DOSWALD-BECK, *Customary International Humanitarian Law Volume II: Practice* (Cambridge, 2005).
- V MARCHETTI & J MARKS, *The CIA and The Cult of Intelligence* (London, Jonathan Cape, 1974).
- B F MELTON JR, *The First Impeachment* (Mercher University Press, 1988).
- J B MOORE, *Digest of International Law* (Washington DC, 1906).
- MOSCA C., SCANDONE G., GAMBACURTA S., VALENTINI M., *I servizi di informazione e il segreto di Stato* (Giuffré, Milano, 2008).
- L OPPENHEIM, *International Law* (8th edn, H Lauterpacht, 1955).
- J PERSICO, *Casey: from the OSS to the CIA* (New York, Viking edn, 1990).
- N PETERSEN, *American Intelligence: 1775-1990: A Bibliographical Guide* (Claremont, Regina Books edn, 1992).
- D A PHILLIPS, *The Night Watch* (Ballantine Books, 1977).
- Presidenza del Consiglio dei Ministri – DIS, *Il linguaggio degli Organismi Informativi* (De Luca Editori, 2009).
- M HERMAN, *Intelligence Services in the Information Age: Theory and Practice* (Frank Cass London 2001).
- W S HOLDSWOTH, *A History of English Law Vol. IX* (London, 1924).
- D S KRIS & D WILSON, *National Security Investigations and Prosecutions* (Thomson/West Publ'g, 2007).
- R PROVOST, *International Human Rights Law and Human Rights* (Cambridge University Press, 2003).
- RONZITTI N., *Diritto Internazionale dei Conflitti Armati* (Giappichelli, 4a edn, 2011).
- RONZITTI N., *Introduzione al Diritto Internazionale* (Giappichelli, 4a edn, 2013).
- ROZO ACUÑA E., *Habeas Data costituzionale: nuova garanzia costituzionale del diritto pubblico latinoamericano,* in *Diritto pubblico comparato ed europeo* (Giappichelli, Torino, 2002-IV).

- ROZO ACUÑA E., voce *Habeas Corpus (America Latina)*, nel *Digesto IV ed., Disc. pen.*, Aggiornamento I, Utet, 2005.
- RUSSO S., *Manuale di Diritto Comunitario dell'Informatica* (Giuffrè, edn, 2010).
- RUSSO S., *Habeas Data e Informatica* (Giuffrè, edn, Milano).
- M SASSOLI, A A BOUVIER, A QUINTIN, *How Does Law Protect in War?* (ICRC, 3rd edn).
- D B SILVER, F P HITZ & J E SHREVE ARIAIL, *Intelligence and Counterintelligence*, in *National Security Law* (J N Moore & R F Turner, 2nd edn, 2005).
- J SIMS, *U.S Intelligence at the Crossroads: Agendas for Reform* (Roy Godson & al edn, 1995).
- Sistema di Informazione per la Sicurezza della Repubblica, *Le Informazioni per la Sicurezza in un Sistema Democratico – Quaderno di Intelligence 1* (De Luca Editori d'Arte edn, 2013).
- Sistema di Informazione per la Sicurezza della Repubblica, *Le Informazioni per la Sicurezza in un Sistema Democratico – Quaderno di Intelligence 2* (De Luca Editori d'Arte edn, 2013).
- J B SMITH, *Portrait of a Cold Warrior* (Ballantine Books, 1976).
- SS8 NETWORKS, *The Ready Guide to Intercept Legislation II* (2007): www.ss8.com.
- A THEOHARIS, *From the Secret Files of J. Edgar Hoover*, Memorandum from Attorney General Howard McGrath for J. Edgar Hoover, Dir. (Ivan R. Dee, Inc. 1933).
- Verizon Enterprise Solutions, "Verizon Data Breach Investigation Report" [2014]: http://www.verizonenterprise.com/it/DBIR/2014/.
- Q WRIGHT, J STONE, R A FALK & R J STANGER, *Essays on Espionage and International Law* (Ohio State University Press, 1962).

ARTICOLI

- T ABBAS, “U.S. Preservation Requirements and EU Data Protection: Headed for Collision?” (2013) 36 Hastings Int'l & Comp L Rev 257-288.
- K W ABBOTT, “«Trust but Verify»: The Production of Information in Arms Control Treaties and Other International Agreements” (1993) 26 Cornell Int’l L J 1-50.
- G H ALDRICH, “Questions of International Law Raised by the Seizure of the U.S.S. Pueblo” 63 Am Soc'y Int'l L Proc 2-6.
- ANONIMO, “United States: Telecommunications - Data Protection” (2006) 12 C T L R 147-148.
- ANSALONE G, *Cyber-spazio e Nuove Sfide alla Sicurezza* in IAI Rivista Online, 2010: http://www.affarinternazionali.it/articolo.asp?ID=1606.
- ANZON A., *Il segreto di Stato, ancora una volta tra stato e costituzione*, in Giur. Cost., 1976.
- L R ATKINSON, “The Fourth Amendment’s National Security Exceptions: Its History and Limits” (2013) 66 L Vand Rev 1343-1405.
- A ATTERITANO, “Immunity of States and Their Organs: The Contribution of Italian Jurisprudence Over the Past Ten Years” [2009] 19 Italian Y B Int’l L 48-49.
- ARCONZO G., *Il segreto di Stato nella giurisprudenza della Corte Costituzionale e della Corte europea dei diritti dell’uomo*, in AIC rivista telematica, 2012.
- O BANGERTER, “A Collection of Codes of Conduct Issued By Armed Groups” (2011) 882 IRRC 483-501.
- C D BAKER, “Tolerance of International Espionage: A Functional Approach” (2003) 5 American U Int’l L Rev 1091-1113.
- T BAKKEN, “The Prosecution of Newspapers, Reporters, and Sources for Disclosing Classified Information: The Government’s Softening of The First Amendment” (2013) 45 U Tol L Rev 1-28.
- D G BARNUM, “Warrantless Electronic Surveillance in National Security Cases: Lessons From America” (2006) 5 E H R L R 514-540.
- D G BARNUM, “Foreign Intelligence Surveillance in the United States: Update” (2008) 5 E H R L R 633-655.

- G N BARRIE, “Spying – an International Law Perspective” (2008) 2008 J S Afr L 238-254.
- R R BAXTER, “So-Called 'Unprivileged Belligerency': Spies, Guerrillas, and Saboteurs” (1951) 28 Brit Y B Int'l L 323-345.
- N BENTWICH, “Espionage and Scientific Invention” (1909) 10 J Soc Comp Legis n s 243-249.
- BIANCO E., *Così è cambiata l’intelligence in Italia* in 3 Gnosis, Rivista Italiana di Intelligence, 2007, 1-8.
- J T BILLINGS, “European Protectionism in Cloud Computing: Addressing Concerns Over the Patriot Act” (2012-2013) 21 CommLaw Conspectus 211-231.
- BONETTI P., *Aspetti costituzionali del nuovo sistema di informazione per la sicurezza della Repubblica*, in Dir. soc., 2008.
- L BRANDEIS & S D WARREN, “The Right to Privacy” [1890] 4 Harvard L Rev 193-220.
- F BUGNION, “ICRC Action During the II World War” (1997) 317 IRRC.
- J A CACCAMO, “A Comparison and Analysis of Immunities Defenses Raised by Soviet Nationals Indicted Under United States Espionage Laws” (1980) 6 Brook J. Int'l L. 259-288.
- F M CARLIN, “The Data Protection Directive: the Introduction of Common Privacy Standards” (1966) 21 E L R 65-70.
- CARACCIOLO L., *Homo curiosus*, in 7 Limes Rivista Italiana di Geopolitica, 2014, 7-26.
- P CHADWICK, “The Value of Privacy” (2006) 5 E H R L R 495-508.
- S CHESTERMAN, “"We can't spy...if we can't buy!": the privatization of intelligence and the limits of outsourcing "inherently governmental functions"” (2008) 19 E J I L1055-1074.
- S CHESTERMAN, “Secret Intelligence” (2009) Max Planck Encyclopedia of Public International Law, Oxford University Press: http://opil.ouplaw.com/home/EPIL.

- K C CLARK & D BARNETTE, "The Application of the Reporter's Privilege and the Espionage Act to Wikileaks" (2011-2012) 37 U Dayton L Rev 165-183.
- R E COYLE, "Surveillance From the Seas" (1973) 60 Mil L Rev 75-95.
- DAMIS J., *Se il Grande Fratello Spia gli Alleati* in IAI Rivista Online, 2013: http://www.affarinternazionali.it/articolo.asp?ID=2443.
- P DE HERT, "Data Protection in the Case Law of Strasbourg and Luxemburg : Constitutionalisation in Action" (2009) Springer Science 3-44.
- I DELUPIS, "Foreign Warships and Immunity for Espionage" (1984) 78 Am J Int'l L 53-75.
- *G* B DEMAREST, "Espionage in International Law" (1995-1996) 24 Denv J Int'l L & Pol'y 321-348.
- J E DONOGHUE, "Perpetual Immunity for Former Diplomats? A Response to «The Abisinito Affair: A Restrictive Theory of Diplomatic Immunity?»" (1989) 27 Colum J Transnat'l L 615-627.
- K DORMANN, "The Legal Situation of Unlawful/Unprivileged Combatants" (2003) 849 IRRC 45-74.
- M F DOWLEY, "Government Surveillance Powers Under the USA PATRIOT Act: Is It Possible to Protect National Security and Privacy at the Same Time? A Constitutional Tug-of-War" (2002-2003) 36 Suffolk U L Rev 165-183.
- C DROEGE, "The Interplay Between International Humanitarian Law and International Human Rights Law in Situations of Armed Conflict" [2007] 40 Isr L Rev 310-355.
- H EDGAR & B C SCHMIDT JR, "The Espionage Statutes and Publication of Defense Information" [1973] 73 Colum L Rev 967-1036.
- L S EDMONSON, "Espionage in Transnational Law" (1971-1972) 5 Vand J Transnat'l L 434-458.
- T S ELLIS, "National Security Trials: a Judge's Perspective" (2013) 99 Va L Rev 1607-1633.

- R D EPSTEIN, “Balancing National Security and Free-Speech Rights: Why Congress Should Revise the Espionage Act” (*2006-2007)* 15 Comm Law Conspectus 483-516.
- I ERDOGAN, “Economic Espionage as a New Form of War in the Post Cold-War Period” [2009] 2 USAK Yearbook 265-282.
- J C EVANS, “Hijacking Civil Liberties: The USA PATRIOT Act of 2001” (2001-2002) 33 Loy U Chi L J 933-990.
- FAINI M., *Lo Spionaggio Industriale Allarga la Faglia del Pacifico* in 7 Limes Rivista Italiana di Geopolitica, 2014, 77-82.
- D FLECK, “Individual and State Responsibility for Intelligence Gathering” [2007] 28 Mich J Int’l L 687-709.
- H FARRELL & M FINNEMORE, “The End of Hypocrisy – American Foreign Policy in the Age of Leaks” (2013) 92 Foreign Aff 22-26.
- C FORCESE, “Spies Without Borders: International Law and Intelligence Collection” (2011-2012) 5 J Nat'l Sec L & Pol'y 179-210.
- M FRULLI, “Some Reflections on the Functional Immunity of State Officials” [2009] 19 Italian Y B Int’l L 91-99.
- GAETA P., *Extraordinary renditions* e immunità dalla giurisdizione penale degli agenti di Stati esteri: il caso *Abu Omar*, RDI, 2006, p. 126ss.
- GALLO C., Datagate: *Europa Sotto Scacco* in Eurasia-Rivista.org, 2013: http://www.eurasia-rivista.org/datagate-europa-sotto-scacco/20425/.
- M R GARCIA-MORA, “Treason, Sedition and Espionage as Political Offenses Under the Law of Extradition” (1964-1965) 26 U Pitt L Rev 65-97.
- D GRAY & D CITRON: “The Right to Quantitative Privacy” (2013) 98 Minn L Rev 62-144.
- N GRIEF, “The Take-Over of the United States' Embassy in Teheran**:** Some Questions of Diplomatic Law” (1980) 13 B L J 46-56.
- D HARDIN, “The Fuss over Two Small Words: The Unconstitutionality of the USA PATRIOT Act Amendments to FISA Under the Fourth Amendment” (2003) 71 Geo Wash L Rev 291-346.

- J L HESTER, “The Espionage Act and Today’s High-Tech Terrorist” (2010-2011) 12 N C J L & Tech 177-198.
- H P HESTERMEYER, “Vienna Convention and Diplomatic Relations (1961)” [2009] Max Planck Encyclopedia of Public International Law §3(25): http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1004?rskey=TXLvwj&result=2&prd=EPIL.
- M B HOROWITZ & Y Y HAIMES, “Risk-Based Methodology for Scenario Tracking, Intelligence Gathering, and Analysis for Countering Terrorism” (2003) 3 Systems Engeneering 152-169.
- A S HULNICK, “Espionage: Does it Have a in the 21st Century?” (2004-2005) 11 Brown J World Aff 165-173.
- F HUYGHE, “The Impurity of War” (2009) 873 IRRC 21-34.
- K JENNINGS: “Espionage: Anything Goes?” (1986-1987) 14 Pepp L Rev 647-666.
- C J JENSEN III, J L REGENS & N GRIFFIN, “Intelligence-Led Policing as a Tool for Countering the Terrorism Threat” (2013) 7 Homeland Security Rev 265-284.
- L K JOHNSON, “Spies” [Sett 2000] Foreign Pol’y.
- K W KAPITAN, “An Introduction to Intelligence Oversight and Sensitive Information: The Department of Defense Rules for Protecting Americans' Information and Privacy” (2013) 2013 Army Law 3-42.
- N S KHURUSHCHEV, “The "Zakharov-Daniloff Affair," the Diplomatic Expulsions of October 1986, and the Hostile Espionage Threat Facing the United States of America” (1988) 14 Brook J Int'l L 109-145.
- R KOLB, “The Relationship Between International Humanitarian Law and Human Rights Law” [1998] 80 Int’l L Rev Red Cross.
- T KONSTATINIDES, “Destroying Democracy on the Ground of Defending it? The Data Retention Directive, the Surveillance State and Our Constitutional Ecosystem” (2012) 1 European Current Law xi-xxiii.
- P KORODY, “States Surveillance Within U.S. Borders” [2004] 65 Ohio St L J 1627-1672.

- H KRIEGER, “A Conflict of Norms: the Relationship Between Humanitarian Law and Human Rights Law in the ICRC Customary Law Study” [2006] 11 J Conflict & Sec L 265-292.
- M B KRIZEK, “The Protective Principle of Extraterritorial Jurisdiction: a Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice” (1988) 6 B U Int'l L J 337-359.
- J W KROPF, “Networked and Layered: Understanding the U.S. Framework for Protecting Personally Identifiable Information” (2007) World Data Protection Report.
- H M LACEY, “Government Secrets, National Security and Freedom of the Press: The Ability of the United States to Prosecute Julian Assange” (2010-2011) 1 Nat'l Sec & Armed Conflict L Rev 202-226.
- B D LARK, “Diplomatic Immunity-Open-Door Policy to Espionage Activity Avoided” (1986) 7 N Y L Sch J Int'l & Comp L 267-280.
- A LAKATOS, “Analysis of the USA Prism and Other NSA surveillance programs” (2013) 8 Data Protection Law and Policy 8-10.
- Y L LING, “A Comparative Study of the Privileges and Immunities of United Nations Member Representatives and Officials With the Traditional Privileges and Immunities of Diplomatic Agents” [1976] 33 Wash & Lee L Rev 125-155.
- P G MADRIÑAN, “Devil in the Details: Constitutional Problems Inherent in the Internet Surveillance Provisions of the USA PATRIOT Act of 2001” (2002-2003) 64 U Pitt L Rev 783-834.
- P MELL, “Big Brother at the Door: Balancing National Security With Privacy Under the USA PATRIOT Act” (2002-2003) 80 Denv U L Rev 375-427.
- T MERON, “The Humanization of Humanitarian Law” [2000] 94 Am J Int’l L 239-278.
- L MITCHELL, “Secret Agent Man: the Need for a Specialized Court-Martial to Try all Espionage-Related Crimes” (2012-2013) 16 Gonz J Int'l L 1-21.

- B A MOHL, “Conflicts Between National Security and Press Freedom” (1978) 2 Fletcher F 232-237.
- C C MORRISSON, “International Law and the Seizure of the USS Pueblo” (1968) 4 Tex Int'l L F 187-193.
- C F MURPHY JR., “Pueblo, E.C. 121, and Beyond: A Suggested Analysis” (1969-1970) 38 Fordham L Rev 439-454.
- NINO M., *Il caso* Datagate*: problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy* in 7 Diritti Umani e Diritto Internazionale, 2013, 727-746.
- R NORWOOD, “None Dare Call it Treason: the Constitutionality of Death Penalty for Peacetime Espionage” (2001-2002) 87 Cornell L Rev 820-852.
- ORLANDI R., Segreto di Stato e limiti alla sua opponibilità, in Giur. Cost., 2010.
- X H OYARCE, “Pueblo Incident (1968)” [2007] Max Planck Encyclopedia of Public International Law: http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1210?rskey=jONnuq&result=1&prd=EPIL.
- PACE A., *L’apposizione del segreto di Stato nei principi costituzionali e nella legge n. 124 del 2007*, in Giur. Cost., 2008.
- M PAPANDREA, “Balancing and the Unauthorized Disclosure of National Security Information” (2012-2013) 97 Iowa L Rev Bull 94-114.
- M PAPANDREA, “Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment” [2014] 94 B U L Rev 449-465.
- J J PAUST, “The Seizure and Recovery of the Mayaguez” (1975-1976) 85 Yale L J 774-807.
- N PELICAN, “Peacetime Cyber-Espionage: a Dangerous but Necessary Game” (2011-2012) 20 Comm Law Conspectus 363-390.
- R J PELTZ-STEELE, “The New American Privacy” (2012-2013) 44 Geo J Int’l L 365-410.
- C PETA, “Cyber-Security: Current Topic of National Security I” (2013) 2 Pub Sec Stud 66-72.

- C PETA, “Cyber-Security: Current Topic of National Security II” (2013) 2 Pub Sec Stud 22-29.
- T PFANNER, “Military Uniforms and the Law of war” (2004) 853 IRRC 93-124.
- P PILLAR, “Intelligence and US Foreign Policy” (2013) Aff 8 Yale J Int'l 119-125.
- R A PIKOWSKI, “An Overview of the Law of Electronic Surveillance Post September 11, 2001” (2002) 94 Law Libr J 601-620.
- Y POULLET; “EU Data Protection Policy, the Directive 95/46/CE: Ten Years After” [2006] Computer Law & Security Report 206-217.
- N PRUD’HOMME, “Lex Specialis: Oversimplifying a More Complex and Multifaceted Relationship?” [2007] 40 Isr L Rev 355-395.
- J RADSAN, "The Unresolved Equation of Espionage and International Law" (2006-2007) 28 Mich J Int'l L 595-623.
- C RITTWEGER & C DECHAMPS, “Germany and the U.S. NSA Surveillance Scandal: The End of Safe Harbor, Standard Contractual Clauses and Personal Data Transfers to the United States?” (2013) 9 World Data Protection Report 1-5.
- A ROBERTS, “Righting wrongs or wronging rights? The United States and human rights post-September 11” (2004) 15 E J I L 721-749.
- RONZITTI N., *Il Caso Snowden e le Regole dello Spionaggio* in IAI Rivista Online, 2013: http://www.affarinternazionali.it/articolo.asp?ID=2369.
- RONZITTI N., *L’Immunità funzionale degli Organi Stranieri dalla Giurisdizione Penale: il Caso Calipari* in 4 RDI, 2008.
- RONZITTI N., *L’ONU Batte un Colpo su Privacy e Spioni* in IAI Rivista Online, 2013: http://www.affarinternazionali.it/articolo.asp?ID=2478.
- B D ROSEMAN, “Electronic Platform, E-mail and Privacy Issues” [2001] SG016 A L I – A B A 1165, 1166-1167.
- M ROTENBERG & D JACOBS, “Updating the Law of Information Privacy: the New Framework of the European Union” (2013) 36 Harv J L & Pub Pol'y 605-652.

- A P RUBIN, “The Impact of the Pueblo Incident in International Law” (1969-1970) 49 Or L Rev 1-12.
- SALVI G., *La Corte Costituzionale e il segreto di Stato*, in Cass. Pen., 2009.
- A SAVIOU & C CAPATINA BASARABESCU, “The Right to Privacy” (2013) 2013 Annals Constantin Brancusi U Targu Jiu Juridical Series 89-96.
- P M SCHWARTZ, “The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures” (2012-2013) 126 Harv L Rev 1966-2009.
- R D SCOTT, “Territorially Intrusive Intelligence Collection and International Law” (1999) 46 A F L Rev 217-226.
- H SCOVILLE, “Is Espionage Necessary for Our Security?” (1975-1976) 54 Foreign Aff 482-495.
- K SEPURA, “Economic Espionage: The Front Line of a New World Economic War” [1998-1999] 26 Syracuse J Int’l L & Com 127-150.
- M R SHEBELSKIE, “The Major Nicholson Incident and the Norms of Peacetime Espionage” (1985-1986) 11 Yale J Int'l L 521-544.
- S SIMITIS, “From the Market to the Polis: The EU Directive on the Protection of Personal Data” [1995] 80 Iowa L Rev 445-470.
- SPAVENTA A., *La nuova partita a scacchi tra Stati Uniti e Cina* in IAI Rivista Online, 2009: http://www.affarinternazionali.it/articolo.asp?ID=1195.
- G SULMASY & J YOO, “Counterintuitive: Intelligence Operations and International Law” (2006) 28 Mich J Int'l L 625-638.
- C SWIFT, “Privacy Protections and the Surveillance State: Bridging the Transatlantic Divide” (2013) 19 Int T L R 75-77.
- O TENE & J POLONETSKY, “Big Data for All: Privacy and User Control in the Age of Analytics” (2012-2013) 11 Nw J Tech & Intell Prop 240-273.
- M J TEPLINSKY, “Fiddling the Roof: Recent developments in Cybersecurity” (2012-2013) 2 Am U Bus L Rev 225-322.
- R M THOMAS, “The British Official Secrets Acts 1911-1939 and the Ponting case” (Agosto 1986) Crim L Rev 491-510.

- T J THOMPSON, “Toward an Updated Understanding of Espionage Motivation” (2014) 27:1 International Journal of Intelligence and CounterIntelligence, 58-72.
- TREZZA C., “L’ascesa della sicurezza cibernetica” in IAI Rivista Online, 2012: http://www.affarinternazionali.it/articolo.asp?ID=1953.
- N P WARD, “Espionage and the Forfeiture of Diplomatic Immunity” (1977) 11 Int'l L 657-671.
- D WEISSBRODT, “Cyber-Conflict, Cyber-Crime, and Cyber- Espionage” (2013) 22 Minn J Int'l L 347-387.
- J Q WHITMAN, “The Two Western Cultures of Privacy: Dignity Versus Liberty” (2004) Yale Law School Faculty Scholarship 1153-1219.
- R D WILLIAMS, “(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action” (2010-2011) 79 Geo Wash L Rev 1162-1200.
- E P WITIW, “Persona Non Grata: Expelling Diplomats Who Abuse Their Privileges” (1988) 9 N Y L Sch J Int'l & Comp L 345-359.
- G H WOODWARD, “Release of the Crew of the U.S.S. Pueblo” [1969] 8 I L M 198-199.
- Q WRIGHT, “Legal Aspects of the U-2 Incident” [1960] 54 Am J Int’l 836-854.
- M D YOUNG, “United States Government Cybersecurity Relationships” (2012-2013) 8 I S J L P 277-320.

FONTI MULTIMEDIALI

- ACLU, “Privacy Rights in the Digital Age” [2014] ACLU Foundation: https://www.aclu.org/privacyrights.
- *Agreement Between the United Nations and the United States Regarding the Headquarters of the United Nations, Signed June 26, 1947, and Approved by the General Assembly October 31, 1947*.

- ANTISERI D. & SOI A., *Intelligence e Metodo Scientifico* (2014) http://www.sicurezzanazionale.gov.it/sisr.nsf/il-mondo-intelligence/intelligence-e-metodo-scientifico.html.
- E B BAZAN, "The Foreign Intelligence Surveillance Act: an Overview of Selected Issues" [2008] Congressional Research Service 1.
- Commission Staff Working Paper: The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, SEC [2002].
- Commission Staff Working Paper: The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, SEC [2004].
- Commissione Europea – Rappresentanza in Italia: "Dati personali, la moneta dell'era digitale: la Commissaria Reding propone un patto per tutelarli"
  (28/1/2014): http://ec.europa.eu/italia/attualita/primo_piano/giustizia_liberta/reding_tutela_dati_it.htm.
- *Committee of Ministers Declaration on Freedom of Expression and Information* del 1982.
- *Committee of Minister Recommendation on "Access to Information Held by Public Authority"* del 1981.
- Consiglio d'Europa, Assemblea Parlamentare, Comitato per gli Affari Giuridici e i Diritti dell'Uomo, "National security and Access to Information" [24 Giugno 2013] 5.
- Consiglio d'Europa, "Human Rights and the Fight Against Terrorism" (2005) The Council of Europe Guidelines.
- *Convention on the Privileges and Immunities of the United Nations* del 1946.

- L COSTA, "A Brief Analysis of Data Protection Law in Brazil" [2012] Presented to the Consultative Committee of the Convention for Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD).
- Council of Europe, Explanatory Report – Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108).
- Council of the European Union, "EU-US data protection «Umbrella Agreement» - Commission Services Non-Paper on state of play of negotiations" (8761/14) Brussels, 9 April 2014.
- Direttiva per l'attuazione delle disposizioni concernenti la tutela amministrativa delle informazioni coperte da segreto di Stato e degli atti relativi al segreto di Stato, contenute nel DPCM 22 luglio 2011, n. 4, pubblicato sulla G.U. n. 203 del 1° settembre 2011: http://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/direttiva-14-febbraio-2012.html.
- ELECTRONIC FRONTIER FOUNDATION, "International Principles on the Application of Human Rights to Communications Surveillance" (July 10, 2013): https://en.necessaryandproportionate.org/text.
- "Espionage and Foreign Interference" *Canadian Security Intelligence Service*, http://www.csis.gc.calprrts/spng/index-eng.asp.
- European Commission, Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final.
- European Commission, "Data Protection – LIBE Committee Vote Backs New EU Data Protection Rules" (10/2013).
- European Commission, "Protection of Personal Data" (15/5/2014): http://ec.europa.eu/justice/data-protection/.
- European Commission, MEMO/13/1059.
- European Commission, MEMO/14/60.
- European Commission, SPEECH/14/62.

- European Commission, “Viviane Reding calls for a data protection compact for Europe” (2014): http://ec.europa.eu/commission_2010-2014/reding/multimedia/news/2014/01/20140128_en.htm.
- European Parliament – Committee on Civil Liberties, Justice and Home Affairs, “Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens’ fundamental rights and on transatlantic cooperation in Justice and Home Affairs” (2013/2188(INI)) e relativi emendamenti.
- European Parliament – Committee on Civil Liberties, Justice and Home Affairs, “NSA snooping: MEPs table proposals to protect EU citizens' privacy” (12/2/2014).
- *Executive Order* No.13526 – *Classified National Security Information* del 29 Dicembre 2009.
- Federal Trade Commission: http://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.
- SORO A., *Big Data Trasparenza Sorveglianza – Relazione 2013: Discorso del Presidente* [10 Giugno 2014].
- Garante per la protezione dei dati personali, *La protezione dei dati nel cambiamento: Big Data Trasparenza Sorveglianza – Relazione 2013*: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3182545.
- Garante per la Protezione dei Dati Personali, “Privacy "Google & Co. attenti, gli utenti hanno perso la fiducia". Approvare subito il nuovo regolamento in discussione a Bruxelles” (2013): http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2732381.
- GA/SHC/4094, “Third Committee Approves Text Titled ‘Right to Privacy in the Digital Age’, as It Takes Action on 18 Draft Resolutions” (2013): https://www.un.org/News/Press/docs/2013/gashc4094.doc.htm.
- https://wikileaks.org/.

- GIUPPONI T. F., *Servizi di informazione e segreto di Stato nella legge n. 124/2007* in www.forumcostituzionale.it.
- P HUSTINX, "High Level Conference: "Ethical Dimensions of Data Protection and Privacy" Centre for Ethics, University of Tartu / Data Protection Inspectorate" (2013) European Data Protection Supervisor.
- ICRC, "A Collection of Codes of Conduct Issued by Armed Groups" [2011] (93)822 Int Rev Red Cross 483-501.
- ICRC, "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977: Commentary – Restrictions on Operations of medical Aircraft".
- ICRC, "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977: Commentary – Spies".
- ICRC, Risorse Online: http://www.icrc.org/applic/ihl/dih.nsf/TRA/135?OpenDocument&.
- ICRC, Risorse Online: http://www.icrc.org/applic/ihl/dih.nsf/INTRO/195.
- ICRC, Risorse Online: http://www.icrc.org/dih/INTRO/150?OpenDocument.
- ICRC, Risorse Online: http://www.icrc.org/ihl/INTRO/275?OpenDocument.
- ICRC, Risorse Online: http://www.icrc.org/applic/ihl/dih.nsf/Treaty.xsp?documentId=CBEC955A2CE7E0D4C12563140043ACA5&action=openDocument.
- ILC, "Report of International Law Commission to the General Assembly" [1958] 2 Y B Intl'l L Comm 78-138.
- International Principles on the Application of Human Rights to Communications Surveillance (10 Luglio 2013): https://en.necessaryandproportionate.org/take-action/EFA.
- Italian Cyber Security Report, "La Cyber Security in Italia" (2013) http://www.sicurezzanazionale.gov.it/sisr.nsf/sicurezza-in-formazione/la-cyber-security-in-italia.html.

- F LA RUE, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" [2013] A/HRC/23/40.
- F LA RUE, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" [2013] A/HRC/23/40/Corr.1.
- P LEAHY, A SPECTER & C E GRASSLEY, "Interim Report on FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures" (February 2003).
- S MELE, "I principi strategici delle politiche di cybersecurity" (2013) http://www.sicurezzanazionale.gov.it/sisr.nsf/il-mondo-intelligence/principi-strategici-delle-politiche-di-cyber-security.html.
- Memorandum from Attorney General Herbert Brownell for J Edgar Hoover, Dir. [1954] FBI 1.
- OAS, "Joint declaration on surveillance programs and their impact on freedom of expression", issued by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (June 2013): www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1.
- *Official Records of the General Assembly, Thirty-sixth Session, Supplement No. 40* (A/36/40) annex XIX, annex XX.
- OHCHR, *General Comment* No. 16: "Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation)" [1988] HRI/GEN/1/Rev.9 (Vol. I).
- OHCHR, "Safeguard privacy while countering terrorism, says Special Rapporteur"
  (2010): http://www.ohchr.org/EN/NewsEvents/Pages/CounterTerrorismAndPrivacy.aspx.

- OHCHR, “The Right to Privacy in the Digital Age” (2013): http://www.ohchr.org/EN/NewsEvents/Pages/Therighttoprivacyinthedigitalage.aspx.
- OHCHR, “Opening Remarks by Ms. Navi Pillay, United Nations High Commissioner for Human Rights to the Side-event at the 24th session of the UN Human Rights Council How to safeguard the right to privacy in the digital age?” (2013): http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13758&LangID=E.
- P HUSTINX, “High Level Conference: "Ethical Dimensions of Data Protection and Privacy" Centre for Ethics, University of Tartu / Data Protection Inspectorate” (2013) European Data Protection Supervisor.
- Parlamento Europeo, Proposta di Risoluzione Comune (2013/2682(RSP)).
- Parlamento Europeo, Proposta di Risoluzione Comune (2013/2831(RSP)).
- POLITI A., *Intelligence e Sicurezza Nazionale*, (2013) http://www.sicurezzanazionale.gov.it/sisr.nsf/il-mondo-intelligence/intelligence-e-sicurezza-nazionale.html.
- Prassi Italiana di Diritto Internazionale, “Lo Spionaggio a Bordo di Aerei” ISGI: http://www.prassi.cnr.it/prassi/content.html?id=2490.
- Presidenza del Consiglio dei Ministri – Sistema di Informazione per la Sicurezza della Repubblica, “Relazione sulla Politica dell’Informazione per la Sicurezza”.
- Presidenza del Consiglio dei Ministri, “Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica” (2013).
- Presidenza del Consiglio dei Ministri, “Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico” (2013).
- Privacy International (NGO), “Submission for the 2013 United Nations Forum on Business and Human Rights”.
- Progetto di Articoli sulla Responsabilità dello Stato della Commissione del Diritto Internazionale (2001).
- Proposta di Direttiva del Parlamento Europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali

da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati, 25 Gennaio 2012, COM(2012) 10 final.

- Protocollo di Firma Facoltativa alla Convenzione di Vienna sulle Relazioni Diplomatiche del 1961.
- Report of the Select Committee on Intelligence United States Senate, "Meeting the Espionage Challenge: a Review of United States Counterintelligence and Security Programs" (1986) 99-522.
- RASI G., *Il nuovo codice sulla protezione dei dati personali tutela la dignità della persona*, 4 Novembre 2004: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/106024.
- M SCHEININ, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism" [2009] A/HRC/13/37.
- Secretary General, Speeches, Data Protection, Surveillance and Internet Governance: The Human Rights Perspective. Global Media Forum "From Information to Participation", 30 June 2014.
- SORO A., *Datagate: Lettera di Antonello Soro al Presidente del Consiglio dei Ministri, Enrico Letta*, 2013: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/print/2708275**.**
- SORO A., *Datagate occasione per ripensare valore dati personali*, 2013: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2748159.
- Statuto della Corte Internazionale di Giustizia del 26 giugno 1945.
- P ŚWITALSKI, "Snooping on People's Privacy – the Implications of Internet Mass Surveillance on Human Rights" [2013] 11 ALER-T.
- The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS No. 108], Proposition of Modernisation, 18 December 2012.

- The Federal Commissioner for Data Protection and Freedom of Information, "Conference of Data Protection Commissioners says that intelligence services constitute a massive threat to data traffic between Germany and other Countries outside Europe" (24 July 2013): http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870.
- "The National Security Agency and Fourth Amendment Rights": Hearing on S. Res. 21 Before the Select Committee to Study Governmental Operations with Respect to Intelligence Activities [1979] 94 Cong 78-101.
- G E TURNER, "The Threat of Foreign Economic Espionage to U.S. Corporations" [1992] 102d Cong, 2nd Sess., 192.
- United Nations, General Assembly, 53rd session, Third Committee, item 106 of the agenda Statement by the International Committee of the Red Cross (ICRC), "Promotion and Protection of the Rights of Children" (1998).
- US Department of Commerce [2000] OJ L 215/7.
- U.S. Dep't of Justice, "The Attorney General's Guidelines for Domestic FBI Operations" [2008].
- U.S. Dep't of Justice "The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection" (U) [2003].
- R B WALTON, "Letter of the FISA Court President to the Chairman of the U.S. Senate Judiciary Committee Patrick J. Leahy about Certain Operations of the FISA Court", 29 July 2013.

GIURISPRUDENZA INTERNAZIONALE

Mexico/U.S.A. (General Claims Commission)

- *Francisco Mallén (United Mexican States) v. U.S.A.* [1927] 4 Reports of International Arbitral Awards 173-190.

Permanent Court of International Justice

- *Lotus Case* (France v Turkey) Merits [1927] PCIJ.

International Court of Justice

- *Corfu Channel, U.K. v Albania*, (Judgment) [1948] ICJ 15.
- *Case Concerning Diplomatic and Consular Staff in Teheran* (24 May 1980) ICJ.
- *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v United States of America) Merits, Judgment of 27 June 1986, ICJ.
- *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion of 8 July 1996, ICJ Reports 1996(I), ICJ.
- *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion of 9 July 2004, ICJ.
- *Case Concerning Armed Activities on the Territory of the Congo (DRC v. Uganda)* of 19 December 2005, ICJ.

European Court of Human Rights

- *Klass and Others v Germany* (Application no 5029/71) [1978] CEDU.
- *Artico v. Italy* (Application no 6694/74) [1980] CEDU.
- *X and Y v. Netherlands* (Application no 8978/90) [1985] CEDU.
- *Leander v Sweden* (Application no 9248/81) [1987] CEDU.
- *Soering v. United Kingdom* (Application no 14038/88) [1989] CEDU.
- *Costello-Roberts v. United Kingdom* (Application no 13134/87) [1993] CEDU.
- *Amann v Switzerland* (Application no 27798/95) [2000] CEDU.
- *Rotaru v Romania* (Application no 28341/95) [2000] CEDU.
- *Mikulic v Croatia* (Application no 53176/99) [2002] CEDU.
- *Bosphorus Hava Yollari Turizm ve Ticaret Anonim Şirketi v. Ireland* (Application no 45036/98) [2005] CEDU.
- *Segerstedt-Wiberg and Others v Sweden* (App no 62332/00) [2006] CEDU.
- *Guja v. Moldova* (Application no 142774/04) [2008] CEDU.
- *S. and Marper v the United Kingdom* (Applications nos 30562/04 and 30566/04) [2008] CEDU.

- *Gillan and Quinton v the United Kingdom* (Application no 4158/05) [2010] CEDU.
- *Bucur and Toma v. Romania* (Application no 40238/02) [2013] CEDU.

European Commission of Human Rights

- *Treholt v. Norway*, Admissibility Decision [1991] ECiHR 192-194.

(European) Court of Justice

- CGUE, *Lindqvist*, sentenza 6 Novembre 2003, C101-01.
- CGUE, *Österreichischer Rundfunk*, sentenza 20 Maggio 2003, cause riunite C-465/00, C-138/01 e C-139/01.
- CGUE, *Google Spain SL / Google Inc. v. Agencia de Protección de Datos(AEPD), Mario Costeja González*, sentenza 13 Maggio 2014, C-131/12.

Inter-American Commission of Human Rights

- Inter-American Commission of Human Rights, *Coard & al. v. United States*, case No. 10.951, Report No. 109/99 [1999] §§37-43.

GIURISPRUDENZA ITALIANA

- Corte d'Appello di Milano (Sez. III Penale) 1 Febbraio 2013.
- Corte di Cassazione, Cass. Civ., Sez. I, 22 Giugno 1995 n. 3769.
- Corte di Cassazione, Cass. pen., Sez. I, 9 Febbraio 1996 n. 878.
- Corte di Cassazione, Cass. pen., Sez. V, 19 Settembre 2012, n.46340.
- Corte Costituzionale, Sentenza n 38/1973.
- Corte Costituzionale, Sentenza n 82/1976.
- Corte Costituzionale, Sentenza n 86/1977.
- Corte Costituzionale, Sentenza n 139/1990.
- Corte Costituzionale, Sentenza n 110/1998.
- Corte Costituzionale, Sentenza n 410/1998.
- Corte Costituzionale, Ordinanza n 344/2000.

- Corte Costituzionale, Sentenza n 487/2000.
- Corte Costituzionale, Sentenza n 295/2002.
- Corte Costituzionale, Ordinanza n 404/2005.
- Corte Costituzionale, Sentenza n 139/2007.
- Corte Costituzionale, Sentenza n 106/2009.
- Corte Costituzionale, Sentenza n 40/2012.

GIURISPRUDENZA ESTERA

United States of America

- *American Banana Co. v. United Fruit Co.* [1909] 213 U.S. 347.
- *Strassheim v. Daily* [1911] 221 U.S. 280.
- *United States v. Bowman* [1922] 260 U.S. 94.
- *Olmstead v U.S.* [1928] 277 U.S. 438.
- *United States v Curtiss-Wright Exp Corp* [1936] 299 U.S. 304-320.
- *Gorin v United States* [1941] 312 U.S. 19-28.
- *Goldman v. United States* [1942] 316 U.S. 129-135.
- *Berger v. New York* [1967] 388 U.S. 41.
- *Katz v U.S.* [1967] 389 U.S. 347.
- *Ivanov v. United States* [1969] 394 U.S. 165.
- *New York Times Co. v United States* [1971] 403 U.S. 713-714.
- *United States v. United States District Court* [1972] 407 U.S. 297.
- *Vernonia Sch. Dist. 47J v. Acton* [1995] 515 U.S. 646-653.
- *Bartnicki v Vopper* [2001] 532 U.S. 514.
- *United States v Drummond* [1965] 354 F 2d 132.
- *United States v Butenko* [1967] 384 F 2d 554, 556.
- *United States v. Brown* [1973] 484 F 2d 418-426.
- *United States v. Buck* [1977] 548 F 2d 871-875.
- *United States v. Clay* [1970] 430 F 2d 165-170.
- *In re* Sealed Case [2002] 310 F 3d 717-746.

- *In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act [2008] 551 F 3d 1004-1011.
- *Unites States v Sterling* [2013] 724 F 3d 482-499.
- *Ashcroft v. al-Kidd* [2011] 131 S. Ct. 2074-2081.
- *United States v. Jones* [2012] 132 S. Ct. 945-950.
- *United States v. Archer* [1943] 51 F Supp 708.
- *United States v. Coplon* [1949] 84 F Supp 472.
- *United States v. Baker* [1955] 136 F Supp 546.
- *United States v Melekh* [1960] 190 F Supp 67.
- *United States ex rel Casanova v. Fitzpatrick* [1963] 214 F Supp 425-437.
- *United States v. Smith* [1971] 321 F Supp 424-426.
- *United States v. Enger* [1978] 472 F Supp 502.
- United States Foreign Intelligence Surveillance Court, "In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From Verizon Business Network Services, Inc. on Behalf of MCI Communication Services, Inc. D/B/A Verizon Business Services" (4/25/2013).

United Kingdom

- *Dickinson v Del Solar* [1930] 1 KB 376.
- *R v Bow Street Metropolitan Stipendiary Magistrate, ex Parte Pinochet Ugarte* (No 3) [1999] 2 WLR 827, [1999] 2 All ER 97, 119 ILR 135.